[PDF] Snort-lightweight **intrusion detection** for networks
M Roesch - Proceedings of the 13th USENIX conference on ..., 1999 - usenix.org
... 229 Page 3. Snort – Lightweight **Intrusion Detection** for Networks Roesch How Is Snort Different From tcpdump? ... Snort decodes the **application layer** of a packet and can be given rules to collect traffic that has spe- cific data contained within its **application layer**. ...
Cited by 1591 - Related articles - View as HTML - All 43 versions

Intrusion detection in wireless ad-hoc networks
Y Zhang, W Lee - Proceedings of the 6th annual international ..., 2000 - portal.acm.org
... However, **intrusion detection** in the **application layer** is not only feasible, as discussed in the previous section, but also necessary because certain attacks, for example, an attack that tries to create an unauthorized access "back-door" to a service, may seem perfectly legiti- mate ...
Cited by 764 - Related articles - All 43 versions

Intrusion detection techniques for mobile wireless networks
Y Zhang, W Lee, YA Huang - Wireless Networks, 2003 - portal.acm.org
... services. In the wireless networks, there are no firewalls to protect the services from attack. However, **intrusion detection** in the **application layer** is not only feasible, as discussed in the previ- ous section, but also necessary. Certain ...
Cited by 369 - Related articles - BL Direct - All 28 versions

Honeycomb: creating **intrusion detection** signatures using honeypots
C Kreibich, J Crowcroft - ACM SIGCOMM Computer Communication ..., 2004 - portal.acm.org
... The philosophy behind our approach is to keep the system free of any knowledge specific to certain **application layer** protocols ... Available: http://citeseer.nj.nec.com/article/paxson98bro.html [2] M. Roesch, "Snort: Lightweight **Intrusion Detection** for Networks," in Proceedings of the ...
Cited by 326 - Related articles - BL Direct - All 64 versions

Testing network-based **intrusion detection** signatures using mutant exploits
G Vigna, W Robertson, D Balzarotti - ... of the 11th ACM conference on ..., 2004 - portal.acm.org
... One may argue that the **intrusion detection** system may be considered to be the test suite and that the variations of an attack ... Mutation techniques can operate at several layers, the most significant of which are the network layer, the **application layer**, and the exploit layer. ...
Cited by 120 - Related articles - All 27 versions

[PDF] Active platform security through **intrusion detection** using naive bayesian network for anomaly **detection**
AA Sebyala, T Olukemi, L Sacks - London Communications Symposium, 2002 - Citeseer
... There are two main categories of **intrusion detection** techniques; Anomaly **detection** and Misuse **detection**. ... 3.2 Development of Anomaly **detection** system Model ... References [1] Ian W Marshal, ("An architecture for **application layer** active networking", IEE, London, 2000. ...
Cited by 39 - Related articles - View as HTML - All 7 versions

Collaborative **intrusion detection** system (cids): A framework for accurate and efficient ids
YS Wu, B Foo, Y Mei, S Bagchi - 2003 - computer.org
... For this purpose, a system is divided into the network layer, the kernel layer and the application layer. ... We design and implement a system called the Collaborative **Intrusion Detection** System (CIDS) to demonstrate the feasibility of the idea. **...**
Cited by 45 - Related articles - All 11 versions

Learning rules for anomaly **detection** of hostile network traffic
MV Mahoney, PK Chan - ... on Data Mining, 2003. ICDM 2003, 2003 - ieeexplore.ieee.org
... In the university traffic, all of the anomalies are due to idiosyncratic variations, mostly at the **application layer**, for example, generic values in **... [5]** R. Lippmann, JW Haines, DJ Fried, J. Korba, & K. Das (2000), "The 1999 DARPA Off-Line **Intrusion Detection** Evaluation", Computer **...**
Cited by 90 - Related articles - All 40 versions

Denial of service in sensor networks
AD Wood, JA Stankovic - Computer, 2002 - ieeexplore.ieee.org
... nodes. An **intrusion-detection** system monitors a host or network for suspicious activity patterns such as those that match some preprogrammed or possi- bly learned rules about what constitutes normal or abnormal behavior. **2 ...**
Cited by 784 - Related articles - BL Direct - All 10 versions

Operational experiences with high-volume network **intrusion detection**
H Dreger, A Feldmann, V Paxson, R ... - Proceedings of the 11th ..., 2004 - portal.acm.org
... Next we recapitulate a recurring experience: in network **intrusion detection**, one faces a rather unusual trade-off between resource requirements and **...** of state entries differs due to factors such as IP defragmenta- tion, TCP stream reassembly, and **application-layer** analysis, which **...**
Cited by 77 - Related articles - All 24 versions

Protocol analysis in **intrusion detection** using decision tree
T Abbes, A Bouhoula, M ... - ... Technology: Coding and ..., 2004 - ieeexplore.ieee.org
... Finally, as **application layer** protocols can be stacked one on the other, we define in each container the type and the address of the next container which will refer to the next **...** Most **intrusion detection** systems rely on pattern match- ing operations to look for attack signatures. **...**
Cited by 40 - Related articles - All 15 versions

SCIDIVE: a stateful and cross protocol **intrusion detection** architecture for voice-over-IP environments
YS Wu, S Bagchi, S Garg, N Singh, T Tsai - 2004 - computer.org
... Since VoIP systems use multiple **application layer** protocols, horizontal cross-protocol correlation is required. **...** Our goal in the paper is to provide an architecture suited to **intrusion detection** in VoIP systems and show the feasibility of the architecture by demonstrating its behavior **...**
Cited by 66 - Related articles - All 16 versions

Adaptive neuro-fuzzy **intrusion detection** systems
S Chavan, K Shah, N Dave, S Mukherjee, A Abraham, ... - 2004 - computer.org
... a libpcap-based sniffer and logger **[3].** It is a cross- platform, lightweight **intrusion detection** tool that **...** The **detection** engine is programmed using a simple language that describes per packet tests **...** SNORT decodes the **application layer** of a packet and can be given rules to collect **...**
Cited by 35 - Related articles - All 22 versions

Measuring normality in HTTP traffic for anomaly-based **intrusion detection**
JM Estévez-Tapiador, P García-Teodoro, JE Díaz- ... - Computer Networks, 2004 - Elsevier
... 4. A new stochastic approach for anomaly-based **intrusion detection** at the **application layer**. In this section, we present a new stochastic approach intended to improve on the general anomaly-based **intrusion detection** results provided by currently used techniques. **...**

Cited by 35 - Related articles - All 8 versions

Architectures for **intrusion** tolerant database systems
P Liu - Computer Security Applications Conference, 2002. ..., 2002 - ieeexplore.ieee.org
... D Multi-layer **intrusion detection** is usually necessary for **detection** accuracy. First, proofs from **application layer**, session layer, transaction layer, process layer, and system call layer should be synthesized to do in- trusion **detection**. ...
Cited by 100 - Related articles - All 16 versions

Design and implementation of a TCG-based integrity measurement architecture
R Sailer, X Zhang, T Jaeger, L Van ... - Proceedings of the 13th ..., 2004 - portal.acm.org
... to extend the TCG trust measurement concepts to dynamic executable content from the BIOS all the way up into the **application layer**. ... 8. [8] G. Kim and E. Spafford, "Experience with Tripwire: Using Integrity Checkers for **Intrusion Detection**," in System Administration, Networking ...
Cited by 501 - Related articles - All 14 versions

[PDF] PHAD: Packet header anomaly **detection** for identifying hostile network traffic
M Mahoney, PK Chan - Florida Institute of Technology technical report CS ..., 2001 - Citeseer
... Horizon (1998) and Ptacek and Newsham (1998) describe techniques for attacking or evading an **application layer** IDS that would produce anomalies at the layers below. ... For example, in the DARPA **intrusion detection** data set (Lippmann et al. ...
Cited by 99 - Related articles - View as HTML - All 9 versions

Intrusion prevention system design
X Zhang, C Li, W Zheng - 2004 - computer.org
... can not prevent attack coming from **application layer**, and can not prevent virus also. It is a good ideas to integrate isolation function of the firewall with the **detection** function of the IDS, and form a new and powerful network security technology: **Intrusion** Prevention System(IPS ...
Cited by 36 - Related articles - All 5 versions

[PDF] Applying Mobile Agents to **Intrusion Detection** and Response.
WA Jansen, T Karygiannis, DG Marks - 2000 - Citeseer
... One of the greatest benefits of MAs is the implementation of interoperability at the **application layer**. ... COTS interoperability may also be facilitated via the use of Agent Communication Languages (ACL) designed for network security testing and **intrusion detection** domains. ...
Cited by 101 - Related articles - View as HTML - All 47 versions

A specification-based **intrusion detection** system for AODV
CY Tseng, P Balasubramanyam, C Ko, R ... - Proceedings of the ..., 2003 - portal.acm.org
... distributed **intrusion detection** and response framework for MANET. Anomaly **detection** is the primary ID approach discussed, including anomalies in routing updates, abnormalities at the MAC layer (number of channel requests, etc.) and at the mobile **application layer** (number ...
Cited by 139 - Related articles - All 10 versions

[BOOK] Computer **intrusion detection** and network monitoring: a statistical viewpoint
DJ Marchette - 2001 - books.google.com
... The section on **intrusion detection** is split into network and host monitoring. ... Rather than focusing on **detection**, I consider the problem of modeling virus propagation. ... It passes it up to the IP.layer, which passes it to the protocol layer and finally to the **application layer**, where the ...
Cited by 97 - Related articles - Library Search - All 8 versions

DECIDUOUS: decentralized source identification for network-basedintrusions
HY Chang, R Narayan, SF Wu, BM ... - Proceedings of the ..., 1999 - ieeexplore.ieee.org
... ent protocol layers. For example, in DECIDUOUS, it is possible for a network-layer security control protocol (eg, IPSEC) to collaborate with an **application-layer intrusion**

detection system module (eg, IDS for the SNMP engine). **...**
Cited by 50 - Related articles

Learning nonstationary models of normal network traffic for detecting novel attacks
MV Mahoney, PK Chan - Proceedings of the eighth ACM SIGKDD ..., 2002 - portal.acm.org
... Second, an attacker may deliberately use malformed or unusual packets to hide attacks from an IDS **application layer**. **...** Unfortunately, this is a common problem. For example, Handley et. al. [7] studied four commercial **intrusion detection** systems and found that none of them **...**
Cited by 219 - Related articles - All 15 versions

[PDF] Transport and application protocol scrubbing
GR Malan, D Watson, F Jahanian, P Howell - IEEE INFOCOM, 2000 - Citeseer
... Sophisticated attacks can utilize protocol ambiguities be- tween a network **intrusion detection** system and an end-host to slip past the watching NID system **...** Since TCP is a reli- able byte-stream service that delivers its data to the **application layer** in order, both the end-host and **...**
Cited by 70 - Related articles - View as HTML - BL Direct - All 26 versions

Anomaly **detection** in IP networks
M Thottan, C Ji - IEEE Transactions on signal processing, 2003 - ieeexplore.ieee.org
... SNMP is implemented at the **application layer** and runs over the UDP. **...** Statistical analysis has been used to detect both anomalies corresponding to network failures **[5]**, as well as network **intrusions** [6]. Interestingly **...** THOTTAN AND JI: ANOMALY **DETECTION** IN IP NETWORKS **...**
Cited by 186 - Related articles - BL Direct - All 19 versions

Implementing the **intrusion detection** exchange protocol
T Buchheim, M Erlinger, B Feinstein, G ... - ... 2001. ACSAC 2001 ..., 2001 - ieeexplore.ieee.org
... BEEP TCP IP Ethernet, ATM, etc. Figure 2: BEEP's Position in TCP/IP Protocol Stack. 7 **Intrusion Detection** Exchange Protocol (IDXP) **...** When one or more inter- mediate hops are required, the protocol needs to set up an **application-layer** tunnel across those hops. **...**
Cited by 18 - Related articles - All 9 versions

Distributed firewalls
SM Bellovin - Journal of Login, 1999 - usenix.org
... It is most natural to think of this happening at the network or the transport layer, but policies and enforcement can equally well apply to the **application layer**. For example, some sites might wish to force local Web browsers to disable Java or JavaScript. **... Intrusion Detection**. **...**
Cited by 140 - Related articles - All 49 versions

[PDF] Detecting computer and network misuse through the production-based expert system tool (P-BEST)
U Lindqvist, PA Porras - Doktorsavhandlingar vid Chalmers Tekniska ..., 1999 - cs.umbc.edu
... For more than a decade, earlier versions of P-BEST have been used in **intrusion detection** research and in the development of some of the most well- known **intrusion detection** systems, but this is the first time the principles and language of P-BEST are described to a wide **...**
Cited by 271 - Related articles - View as HTML - BL Direct - All 44 versions

Evaluation of the diagnostic capabilities of commercial **intrusion detection** systems
H Debar, B Morin - Recent Advances in **Intrusion Detection**, 2002 - Springer
... Misunderstanding of the protocol states or properties. Sometimes, vul- nerabilities are only applicable to certain states of the **application layer** proto- cols. **...** Sometimes, protocols encode data, hiding the information from the **intrusion-detection** system and inducing false positives. **...**
Cited by 31 - Related articles - BL Direct - All 12 versions

[PDF] Building adaptive and agile applications using **intrusion detection** and response
JP Loyall, P Pal, R Schantz, F Webber - Proc. of NDSS, 2000 - isoc.org

... IDS, and application-specified **intrusion detection** are all integrated to provide **intrusion** awareness and adaptive behavior in response to intru- sion **detection** at the ... interfacing to multiple IDSs, enabling the IDSs to cooperate through the **application layer** and increasing ...
Cited by 22 - Related articles - View as HTML - All 3 versions

[PDF] Live traffic analysis of TCP/IP gateways
PA Porras, A Valdes - NDSS, 1998 - isoc.org
... on or forgery of l egi ti mate tra cin an at- tempt to negativelya ect routing services, **application-layer** services, or ... Continuous measures are useful not onlyfor **intrusion detection**, but alsosupport the monitoringof healthand status of the networkfromthe perspective of connectiv ...
Cited by 114 - Related articles - View as HTML - All 2 versions

Towards nic-based **intrusion detection**
M Otey, S Parthasarathy, A Ghoting, G Li, S ... - Proceedings of the ..., 2003 - portal.acm.org
... As a result, several data stream processing algorithms are rendered inapplicable for network **intrusion detection** un- der real-time processing requirements. ... see figure 2) is loosely based on one of the models used in the non-stationary **application layer** anomaly **detection** (ALAD ...
Cited by 26 - Related articles - All 16 versions

Intrusion detection system for high-speed network
W Yang, BX Fang, B Liu, HL Zhang - Computer Communications, 2004 - Elsevier
... Then, to reduce the data load for **intrusion** analysis, RHPNIDS implements an efficient multi ... Third, an **application-layer** protocol analysis and reassembling mechanism reduce the false alarm rate and ... are designed and implemented as the core of the rule-based **detection** engine. ...
Cited by 15 - Related articles

Passive visual fingerprinting of network attack tools
G Conti, K Abdullah - Proceedings of the 2004 ACM workshop on ..., 2004 - portal.acm.org
... which can be used for such activities as detecting Honeynets[25] and insertion and evasion attacks to bypass **intrusion detection** systems[26]. ... 3.2.1.4 **Application Layer Application layer** headers and data provide a great deal of information about the nature of attacks, but due to ...
Cited by 56 - Related articles - All 9 versions

A model for evaluating IT security investments
H Cavusoglu, B Mishra, S ... - Communications of the ..., 2004 - portal.acm.org
... A packet-filtering mechanism performs filtering based on the set of rules in an access control list. The **Application layer** mechanism uses proxies. ... IDSs attempt to detect **intrusions**. ... IDSs use signature-based or anomaly **detection** approaches. ...
Cited by 144 - Related articles - BL Direct - All 10 versions

Efficient minimum-cost network hardening via exploit dependency graphs
S Noel, S Jajodia, B O'Berry, M ... - ..., 2003. Proceedings. 19th ..., 2003 - ieeexplore.ieee.org
... details). Similarly, we model the combination of **application-layer** trust and physical-layer connectivity as simply **application-layer** trust. ... services. **Application- layer** trust relationships further restrict NFS and NIS domain access. ...
Cited by 120 - Related articles - All 15 versions

Self-organized network-layer security in mobile ad hoc networks
H Yang, X Meng, S Lu - Proceedings of the 1st ACM workshop on ..., 2002 - portal.acm.org
... are the same, and the hop count in the new route entry is one larger than the hop count in the cached route entry announced by Y . If the routing update is not cor- rect, the RREP packet is dropped and node S broadcasts a SID(Single **Intrusion Detection**) packet to its neighbors. ...
Cited by 255 - Related articles - BL Direct - All 24 versions

A dynamic honeypot design for **intrusion detection**

I Kuwatly, M Sraj, Z Al Masri, H ... - IEEE/ACS International ..., 2004 - ieeexplore.ieee.org
... III- RELATED WORK The honeypot technology is an attempt to overcome the shortcomings of **intrusion detection** systems. A. Definition ... KFSensor simulates system services at the **application layer**, thus enabling it to use Windows security mechanisms and libraries. ...
Cited by 22 - Related articles - All 8 versions

Sleepy watermark tracing: An active network-based **intrusion** response framework
X Wang, DS Reeves, SF Wu, J ... - ... {IFIP/Sec'01}, June 11-13, ..., 2001 - books.google.com
... Therefore, watermark belongs to the **application layer** and is application-specific. ... 380 Part Nine Network Security and **Intrusion Detection** " See me" We define a virtual null string of a network application as a string that appears null to end users of the network application. ...
Cited by 88 - Related articles - All 27 versions

Shield: Vulnerability-driven network filters for preventing known vulnerability exploits
HJ Wang, C Guo, DR Simon, A ... - Proceedings of the 2004 ..., 2004 - portal.acm.org
... To this end, we have de- signed a Shield framework that lies between the **application layer** and the transport layer and ... session, and performs application-message-based inspection rather than packet-level inspection, as used by some Network **Intrusion Detection** or Prevention ...
Cited by 230 - Related articles - BL Direct - All 36 versions

A fast string-matching algorithm for network processor-based **intrusion detection** system
RT Liu, NF Huang, CH Chen, CN Kao - ACM Transactions on ..., 2004 - portal.acm.org
... The increase in network utilization and the weekly expansion in number of critical **application layer** exploits means NIDSs designers must develop ways to accelerate their attack analysis techniques when ... String-Matching Algorithm for Network **Intrusion Detection** System • 617 ...
Cited by 60 - Related articles

Interfacing trusted applications with **intrusion detection** systems
M Welz, A Hutchison - Recent Advances in Intrusion Detection, 2001 - Springer
... Most network-based **intrusion detection** systems make use of this method. ... An example of such a system would be the **application layer** proxies of TIS's firewall toolkit [19] or the audit trail of an operating system which records the system calls made by an application. ...
Cited by 20 - Related articles - BL Direct - All 8 versions

[PDF] Application of Belief-Desire-Intention agents in **intrusion detection** and response
M Shajari, AA Ghorbani - Proceedings of Privacy, Security, Trust (PST04) ..., 2004 - Citeseer
... An Agent **Application Layer** Communication Protocol (AALCP) is designed as a protocol for agent communication. The **Intrusion Detection** Agent system (IDA) [15] developed by the Information Technology Promotion Agency (IPA) in Japan is an example of prototypes that use ...
Cited by 11 - Related articles - View as HTML - All 8 versions

Web application security assessment by fault injection and behavior monitoring
YW Huang, SK Huang, TP Lin, CH ... - Proceedings of the 12th ..., 2003 - portal.acm.org
... Since a malicious script that is capable of attacking an interacting browser is also capable of attacking the crawler, a secure execution environment (SEE) that enforces an anomaly **detection** model was built around the crawler. ...
Cited by 135 - Related articles - All 11 versions

[PDF] Providing robust and ubiquitous security support for mobile ad-hoc networks
H Luo, J Kong, P Zerfos, S Lu, L Zhang - IEEE ICNP, 2001 - Citeseer
... The assumption of local de- tection mechanisms is based on the observation that although **intrusion detection** in ad hoc networks is generally ... network layer Smurf and Teardrop, transport layer TCP flooding and SYN flooding, and numerous attacks in the **application layer** [15]. ...
Cited by 579 - Related articles - View as HTML - All 29 versions

Anomaly **detection** methods in wired networks: a survey and taxonomy
JM Estevez-Tapiador, P Garcia-Teodoro, JE ... - Computer ..., 2004 - Elsevier
... Case study V: specification-based protocol anomaly **detection** 6. **Application-layer** anomaly **detection**: payload inspection 6.1. **...** Within the context of network security, anomaly **detection** is one of two fundamental approaches used in **intrusion detection** (ID) technology [4] and [9 **...**
Cited by 44 - Related articles - All 6 versions

[PDF] Stopping intruders outside the gates
LD Paulson - Computer, 2002 - Infolib.hua.edu.vn
... detection to recognize threats based on their behavior, said Raanan **...** said, combining network and host-spe- cific IPSs provides the best protection against all types of **intrusions**. **...** company's vice president of mar- keting, said 80 percent of attacks orig- inate in the **application layer**. **...**
Cited by 20 - Related articles - View as HTML - BL Direct - All 6 versions

A framework for malicious workload generation
J Sommers, V Yegneswaran, P ... - Proceedings of the 4th ..., 2004 - portal.acm.org
... benchmarking tool that enables as- sessment of quality of service degradation (the effect of mal- traffic on good traffic) and resilience of middleboxes and network **intrusion detection** systems (NIDS) over a **...** These could either be at the network layer or at the **application layer**. **...**
Cited by 42 - Related articles - All 17 versions

[PDF] **Intrusion detection** system (IDS) product survey
KA Jackson - Los Alamos National Laboratory, Los Alamos, NM, ..., 1999 - Citeseer
... 06/25/99 **INTRUSION DETECTION** SYSTEM (IDS) PRODUCT SURVEY **...** ii Version 2.1 4.10 REACTIVE **INTRUSION DETECTION** ..... 65 4.11 REALSECURE..... **...**
Cited by 42 - Related articles - View as HTML - All 9 versions

[PDF] Design and implementation of a string matching system for network **intrusion detection** u FPGA-based bloom filters
S Dharmapurikar, M Attig, J Lockwood - ... University in St. Louis, Tech. Rep ..., 2004 - Citeseer
... For applications like network **intrusion detection**, these updates are relatively less frequent than the actual query process it- self. **...** Packets on the link are parsed by the protocol wrappers [2] and the **application layer** data is presented to the scanner module. **...**
Cited by 31 - Related articles - View as HTML - All 8 versions

Dynamic signature inspection-based network **intrusion detection**
V Vaidya - US Patent 6,279,113, 2001 - Google Patents
... the security platform described above provides a partial solution to the network security problem by enabling **detection** of unauthorized access attempts which are based in the **application layer** of the OSI model, the security platform is unable to detect network **intrusions** 10 15 **...**
Cited by 14 - Related articles

An environment for security protocol **intrusion detection**
A Yasinsac - Journal of Computer Security, 2002 - IOS Press
... way. The security of the information provided by trusted services at the **application layer** is dependent on security protocols. **...** We begin by giving the background work in security protocol verification and **intrusion detection**. The **...**
Cited by 12 - Related articles - BL Direct - All 9 versions

Anomaly **intrusion detection** in dynamic execution environments
H Inoue, S Forrest - Proceedings of the 2002 workshop on New ..., 2002 - portal.acm.org
... We call this approach "dynamic sandboxing." By gathering information about applications' behavior usually unavail- able to other anomaly **intrusion-detection** systems, dynamic sandboxing is able to detect anomalies at the **application layer**. **...**
Cited by 24 - Related articles - All 9 versions

[CITATION] The design of a distributed network **intrusion detection** system IA-NIDS
Q Xue, LL Guo, JZ Sun - Machine Learning and Cybernetics, ..., 2003 - 万方数据资源系统
Cited by 8 - Related articles

[PDF] A novel approach to **detection** of denial-of-service attacks via adaptive sequential and ba sequential change-point **detection** methods
RB Blazek, H Kim, B Rozovskii, A ... - Proceedings of the IEEE ..., 2001 - cams.usc.edu
... Existing **intrusion detection** systems can be classified as either Signature **Detection** Systems or Anomaly ... The cor- responding **detection** method will be called the Batch– Sequential Method. III. ... In the **application layer** it is assumed to observe information about packets associated ...
Cited by 69 - Related articles - View as HTML - All 5 versions

[BOOK] **Intrusion detection** systems with Snort: advanced IDS techniques using Snort, Apache MySQL, PHP, and ACID
RU Rehman - 2003 - books.google.com
... Page 21. What is **Intrusion Detection**? 7 1.1.1.4 Signatures Signature is the pattern that you look for inside a data packet. ... For example, you can find signatures in the IP header, transport layer header (TCP or UDP header) and/or **application layer** header or payload. ...
Cited by 31 - Related articles - All 4 versions

Honeypot: a supplemented active defense system for network security
F Zhang, S Zhou, Z Qin, J Liu - Proceedings of the Fourth ..., 2003 - ieeexplore.ieee.org
... The third layer is log component which logs all the activities of the honeypot OS in **application layer**. Log ... attacks. The other contribution to **intrusion detection** is that it can reduce both false positive rate and false negative rate. ...
Cited by 18 - Related articles - All 3 versions

HMM profiles for network traffic classification
C Wright, F Monrose, GM Masson - ... of the 2004 ACM workshop on ..., 2004 - portal.acm.org
... Figure 3 shows that, in the traffic we analyzed, all **application-layer** protocols exhibit significant autocorre- lation in their inter-arrival times ... classifiers, exam- ining FTP, SMTP, HTTP, and Telnet sessions using the data from the MIT Lincoln Labs **Intrusion Detection** Evaluation [13]. ...
Cited by 47 - Related articles - All 3 versions

Network **Intrusion Detection** Techniques Based on Protocol Analysis [J]
JRLLH Jinpeng - Computer Engineering and Applications, 2003 - en.cnki.com.cn
... an **intrusion detection** technique that takes full advantage of the protocol state information for detecting **intrusion**.It can effectively analyze protocols at various layers of network including **application layer** protocols and can accurately locate the field of **detection**,which enhances ...
Cited by 6 - Related articles - Cached

[PDF] Detecting novel attacks by identifying anomalous network packet headers
M Mahoney, P Chan - Florida Institute of Technology Technical Report ..., 1999 - Citeseer
... We got good performance because the important fields for **intrusion detection** have a small r, so ... Tables 5.2 and 5.3 list the unofficial **detection** rates for PHAD-C32, the best ... according to our unofficial classification) are shown in parenthesis, with the **application layer** protocol that ...
Cited by 43 - Related articles - View as HTML - All 8 versions

Visualisation for **Intrusion Detection**
S Axelsson - Computer Security–ESORICS 2003, 2003 - Springer
... network traffic and alarms from a network of **intrusion detection** sensors as glyphs onto a stylised map of the network. As such their approach is very different from ours, in that we don't map the traffic as such, but rather try and visualise meta data from the **application layer** in a ...
Cited by 25 - Related articles - BL Direct - All 11 versions

[PDF] Scampi-a scaleable monitoring platform for the internet
J Coppens, E Markatos, J Novotny, M ... - Proceedings of the 2nd ... , 2004 - Citeseer
... The monitoring layer, belonging to a single Internet Service Provider (ISP), provides end-to-end QoS statistics of the observed network to the **application layer**. ... NDISs (Network **Intrusion Detection** Systems) are an important part of any modern network security architec- ture. ...
Cited by 26 - Related articles - View as HTML - All 13 versions

[PDF] Bro: An open source network **intrusion detection** system
R Sommer - Proceedings of the 17. DFN-Arbeitstagung über ..., 2003 - Citeseer
... On the **application layer**, it implements a variety of protocol-specific analyzers, eg for HTTP, SMTP, DNS and many others. ... The policy layer evaluates the events according to user-supplied scripts. Events are central to Bro's approach to network **intrusion detection**. ...
Cited by 11 - Related articles - View as HTML - All 6 versions

Models for monitoring and debugging tools for parallel and distributed software
DC Marinescu, JE Lumpp Jr, TL Casavant, HJ ... - Journal of Parallel and ..., 1990 - Elsevier
... will be built up from a standard library of functions to support the current **Application layer**, while the **Application layer** will be ... 178 mappings of implementations onto the layered model are given: a nonintrusive system, and an intrusive system demonstrating **detection intrusion**. ...
Cited by 83 - Related articles - All 7 versions

[PDF] GRIP: A reconfigurable architecture for host-based gigabit-rate packet processing
P Bellows, J Flidr, T Lehman, B Schott, KD ... - Proc. of the IEEE ..., 2002 - Citeseer
... reconfigurable comput- ing. These range from **intrusion detection** at the link layer and encryption at the network layer (IPSec) to protocol pro- cessing at the transport layer and parallel computing at the **application layer**. The goal of ...
Cited by 32 - Related articles - View as HTML - All 12 versions

[PDF] Boundary **detection** in tokenizing network application payload for anomaly **detection**
R Vargiya, P Chan - Workshop on Data Mining for Computer Security, 2003 - Citeseer
... are statistical, our approach is independent of the language or in our case, independent of the protocol of the **application layer**. ... 4.2 Evaluation Data and Procedures The proposed methods were evaluated using the 1999 DARPA **Intrusion Detection** Evaluation Data Set [7]. The ...
Cited by 25 - Related articles - View as HTML - All 3 versions

[PDF] Design of an **intrusion**-tolerant **intrusion detection** system
M Dacier... - Research Report, Maftia Project, 2002 - Citeseer
... Malicious- and Accidental-Fault Tolerance for Internet Applications Design of an **Intrusion**-Tolerant **Intrusion Detection** System M. Dacier (Editor) IBM Zurich Research Laboratory ... Page 3. Design of an **intrusion**-tolerant **intrusion detection** system i Table of contents ...
Cited by 24 - Related articles - View as HTML - All 5 versions

A novel distributed **intrusion detection** model based on mobile agent
S Zhicai, J Zhenzhou, H Mingzeng - Proceedings of the 3rd ..., 2004 - portal.acm.org
... as an **application-layer** proxy. It allows authorized users to access services through a firewall. So two different subnet monitors can exchange message safely. These BEEP protocols are called by the communication control module of IDSs. So **intrusion detection** entities can ...
Cited by 10 - Related articles - All 2 versions

Detecting anomalous network traffic with self-organizing maps
M Ramadas, S Ostermann, B Tjaden - ... Advances in Intrusion Detection, 2003 - Springer
... For this, the signature-based **intrusion detection** system SNORT is run on the dumpfile, and ... resulting in the DNS exploit being successfully classified with our **intrusion** threshold of 2 ... The HTTP Tunnel program creates **application-layer** HTTP tunnels between two hosts, and lets ...
Cited by 89 - Related articles - BL Direct - All 46 versions

The Evolution of **Intrusion Detection** Systems--The Next Step
R Barber - Computers & Security, 2001 - Elsevier
... Nobody is suggesting that the solution is perfect or that **Intrusion Detection** Systems are complete as they **...** This partnership also opens the door for a further improvement in **detection** rates and **...** It should also be able to detect and prevent **application layer** attacks that should be **...**
Cited by 11 - Related articles - All 5 versions

Issues in high-speed internet security
P Jungck, SSY Shim - Computer, 2004 - computer.org
... the port it attacked open to provide a service, and most **intrusion detection** systems left **...** might lock out valid SQL communications, and antivirus and **intrusion** protection systems **...** Full packet inspection involves fully interrogating the additional **application layer** headers and making **...**
Cited by 28 - Related articles - BL Direct - All 8 versions

[PDF] De ning an adaptive software security metric from a dynamic software failure tolerance measure
J Voas, A Ghosh, G McGraw, F Charron, K ... - Reliable Software ..., 1996 - Citeseer
... Even patching this flaw in sendmail does not solve the problem of intrud- ers using other non-standard mail headers or exploiting other **application-layer** program vulnerabilities. **... Intrusion detection** will be accomplished using a predicate-based **intrusion** specifi- cation language. **...**
Cited by 48 - Related articles - View as HTML - All 10 versions

[PDF] Optimizing pattern matching for **intrusion detection**
M Norton - white paper, Sourcefire Inc, 2004 - Citeseer
... NORT is an open source **Intrusion Detection** System that relies heavily on the Aho-Corasick multi-pattern search engine. **...** searching for intruders by looking for specific values in the network headers and by performing a search for known patterns in the **application layer** data. **...**
Cited by 37 - Related articles - View as HTML - All 2 versions

Anomaly Network **Intrusion Detection** System Based on Data Mining [J]
S Shi-jie, HU Hua-ping, HU Xiao-lei, JIN Shi ... - Computer ..., 2003 - en.cnki.com.cn
... normal patterns, comparing current system or user behaviors with history behaviors, and then detecting **intrusion**. **...** the process of data mining application in anomaly NIDS from network layer and **application layer**. **...** 【Key Words】 : data mining anomaly **detection** association rules **...**
Cited by 5 - Related articles - Cached

[PDF] Linux security module framework
C Wright, C Cowan, J Morris, S Smalley, G Kroah ... - Ottawa Linux ..., 2002 - Citeseer
... The netlink_send () hook is used to store the **application layer** security state. The netlink_recv () hook is used to retrieve the stored security state as the packet is received by the destination kernel module and mediate final delivery. **...** LIDS (Linux **Intrusion Detection** Sys- tem **...**
Cited by 47 - Related articles - View as HTML - All 45 versions

[BOOK] Designing network security
M Kaeo - 1999 - portal.acm.org
... Part of writing for an audience is keeping the audience's interest. The author clearly explains the difference between **application layer** security protocols, transport layer security protocols, and security protocols found in other layers. **...**
Cited by 72 - Related articles - Library Search - All 7 versions

A sequential pattern mining algorithm for misuse **intrusion detection**
SJ Song, Z Huang, HP Hu, SY Jin - Grid and Cooperative Computing– ..., 2004 - Springer
... Abstract. This paper presents a sequential pattern mining algorithm for misuse **intrusion detection**, which can be used to detect **application layer** attack. **...** But detecting R2L and U2R **application layer** attacks is the main focus of **intrusion detection** re- search at present. **...**

Cited by 5 - Related articles - BL Direct - All 4 versions

[PDF] Detecting **intrusions** in security protocols
A Yasinsac - ... of first workshop on **Intrusion Detection** Systems, in the ..., 2000 - Citeseer
... way. The security of the information provided by trusted services at the **application layer** is dependent on security protocols. ... We begin by giving the background work in security protocol verification and **intrusion detection**. The ...
Cited by 12 - Related articles - View as HTML - All 8 versions

Accurate buffer overflow **detection** via abstract payload execution
T Toth, C Kruegel - ... on Recent advances in **intrusion detection**, 2002 - portal.acm.org
... We have chosen to place our sensor at the **application layer** to circumvent the problem of encrypted network traffic faced by NIDS. ... 2. Debra Anderson, Thane Frivold, Ann Tamaru, and Alfonso Valdes. Next Genera- tion **Intrusion Detection** Expert System (NIDES). ...
Cited by 135 - Related articles - BL Direct - All 8 versions

Accurate, scalable in-network identification of p2p traffic using application signatures
S Sen, O Spatscheck, D Wang - Proceedings of the 13th ..., 2004 - portal.acm.org
... has been mainly performed in the context of network security such as **intrusion** and anomaly ... traces (eg, [9]); however, none of these works provides and evaluates **application layer** P2P signatures. ... Section 4 derives the actual signatures used for P2P **detection**, and Section 5 ...
Cited by 434 - Related articles - All 28 versions

A framework for analyzing e-commerce security
S Kesh, S Ramanujan, S Nerur - Information Management and ..., 2002 - emeraldinsight.com
... Host-based **intrusion detection** systems parse system logs and monitor user logins. ... Because of this, it is transparent to all users. While many applications may have their own security protocols, IPsec works at the network layer and can work with the **application layer** protocols. ...
Cited by 23 - Related articles - BL Direct - All 7 versions

[PDF] The use of attack trees in assessing vulnerabilities in SCADA systems
EJ Byres, M Franz, D Miller - International Infrastructure Survivability ..., 2004 - ida.liu.se
... These systems were selected as a starting point since their underlying **application layer** protocol is both one ... Furthermore, **detection** of this type of attack is highly unlikely as few SCADA systems deploy any form of **intrusion detection** system and the direct impact to operations ...
Cited by 26 - Related articles - View as HTML - All 8 versions

Characteristics of role-based access control
V Gligor - Proceedings of the first ACM Workshop on Role-based ..., 1996 - portal.acm.org
... This is possible because **intrusion detection** would also have to be performed at the same low level as that of access control administration. ... [HAM1921 Deborah Hamilton, "**Application Layer** Security Requirements of a Medical Information System," Proceedings of the 15th NIST ...
Cited by 29 - Related articles - All 2 versions

[PDF] Active mapping: Resisting NIDS evasion without altering traffic
U Shankar, V Paxson - Computer, 2002 - Citeseer
... Page 4. Contents 1 Introduction 1 1.1 The State of Network **Intrusion Detection** . . . . . 1 1.2 Active Mapping . . . ... 30 iii Page 6. Abstract A critical problem faced by a Network **Intrusion Detection** System (NIDS) is that of ambiguity. ...
Cited by 107 - Related articles - View as HTML - BL Direct - All 30 versions

[PDF] The Gigascope stream database
C Cranor, T Johnson, O Spatscheck, V Shkapenyuk - Data Engineering, 2003 - Citeseer
... period, usually only the network protocol headers are stored, which frustrates analyses which use the **application layer** headers of the ... **Intrusion detection**: Network **intrusion detection** can be

accomplished by expressing **intrusion** rules as GSQL queries and feeding the result ...
Cited by 40 - Related articles - View as HTML - All 20 versions

Packet trace manipulation rramework for test labs
A Rupp, H Dreger, A Feldmann, R ... - Proceedings of the 4th ..., 2004 - portal.acm.org
... All other operations disturb the relationships between flows at the **application-layer**: consider a protocol such as FTP which uses a ... 6. SUMMARY Motivated by the task of evaluating Network **Intrusion Detection** Systems, we identify a set of trace manipulating operations that aid ...
Cited by 16 - Related articles - All 21 versions

[PDF] Survivability-over-security: Providing whole system assurance
W Yurcik, D Doss, H Kruse - Information Survivability Workshop, 2000 - Citeseer
... Applications and **application-layer** protocols have been found to interact in unexpected ways with these new layer-violating (LV) network devices (which break the end-to-end model) such as network address translators, firewalls, proxies, **intrusion detection**, and differentiated ...
Cited by 11 - Related articles - View as HTML - All 6 versions

Dissecting Snort, tool for **intrusion detection** [J]
QI Jian-dong, TAO Lan, SUN Zong- ... - Computer Engineering and ..., 2004 - en.cnki.com.cn
... Hunan University, Changsha 410082;The Research of Multi-pattern Matching Algorithm in Network **Intrusion Detection** System[J ... Engineering,Jiangsu University,Zhenjiang 212013,China);Research and implement of honeypot framework for **application layer's** unknown attacks[J ...
Cited by 5 - Related articles - Cached

[PDF] Defining digital forensic examination and analysis tools
B Carrier - Digital Research Workshop II, 2002 - Citeseer
... ASCII .H TML Files . Windows Registry . Network Packets . **Intrusion Detection** System (IDS)alerts . Source Code ... The second layer is the file system layer that translates the sector contents to files. The third layer is the **application layer** that translates the file content to 5 Page 6. ...
Cited by 69 - Related articles - View as HTML - All 33 versions

[PDF] A new vision for network architecture
D Clark - private communication, September, 2002 - ginkgo-networks.com
... The simplicity of the core allows new applications to be deployed at will, but mean that the core cannot detect when problems arise at the **application layer**. ... So trust can be both exploited and validated across applications. Knowledge-based **intrusion detection** ...
Cited by 13 - Related articles - View as HTML - All 5 versions

[PDF] Coordination of security levels for Internet architectures
EB Fernandez - Procs. 10th Intl. Workshop on Database and Expert ..., 1999 - Citeseer
... Current systems incorporate a variety of mechanisms to thwart attackers, eg, cryptographic protocols, **intrusion detection** methods, authorization systems, etc. ... These protect the data at a granularity that can cover specific data values. At the **application layer** we can define ...
Cited by 18 - Related articles - View as HTML - All 5 versions

Efficacy of misuse **detection** in ad hoc networks
D Subhadrabandhu, S Sarkar, F ... - 2004 First Annual IEEE ..., 2004 - ieeexplore.ieee.org
... An obvious IDS placement strategy (host **intrusion detection** or HID) [16] for adhoc networks is to execute the IDS at only the destinations of the sessions, eg destinations 1, 2 in figure 1. Here, a node executes the IDS at its **application layer**, and can therefore analyze only the ...
Cited by 17 - Related articles - All 9 versions

[PDF] What do we mean by Network Denial of Service
C Shields - Proceedings of the 2002 IEEE Workshop on ..., 2002 - Citeseer
... Needham was the first to examine the effects of denial- of-service attacks at the **application layer**,

focusing pri- marily on end-to-end solutions ... denial-of-service at- tacks was taken by Ptacek and Newsham [30] in their dis- cussion of methods of foiling **intrusion detection** systems. ...
Cited by 34 - Related articles - View as HTML - All 5 versions

Self-securing ad hoc wireless networks
H Luo, P Zerfos, J Kong, S Lu, L ... - ... on Computers and ..., 2002 - ieeexplore.ieee.org
... Each node is equipped with some local **detection** mech- anism to identify misbehaving nodes ... This assump- tion is based on the observation that although **intrusion** de- tection in ... Teardrop, transport layer TCP flood- ing and SYN flooding, and various attacks in **application layer**. ...
Cited by 314 - Related articles - All 21 versions

Trust-based routing for ad-hoc wireless networks
AA Pirzada, A Datta, C ... - 12th IEEE International ..., 2004 - ieeexplore.ieee.org
... However, as the routes retrieved from the cache are based the **application layer** of source nodes. upon a minimal trust threshold, we see a control packet ... We recommend using **Intrusion Detection** systems such as those proposed hy Zhang et al. [14] and Kachirski et al. ...
Cited by 30 - Related articles

Timing-sync protocol for sensor networks
S Ganeriwal, R Kumar, MB Srivastava - Proceedings of the 1st ..., 2003 - portal.acm.org
... The applications envisioned for sensor networks vary from monitoring inhospitable habitats and disaster areas to operating indoors for **intrusion detection** and equipment ... There is time spent in actually constructing the packet at the **application layer**, after which it is passed to the ...
Cited by 863 - Related articles - All 42 versions

[PDF] Attack-Class-Based Analysis of **Intrusion Detection** Systems
D Alessandri - ... of Newcastle upon Tyne, Newcastle, UK, 2004 - homepage.swissonline.ch
... **Intrusion Detection** Systems Dominique Alessandri May 2004 ... Page 3. Abstract Designers of **intrusion detection** systems are often faced with the problem that their design fails to meet the specification because the actual implementation is not able to detect attacks as required. ...
Cited by 14 - Related articles - View as HTML - All 2 versions

[PS] Live Tra c Analysis of TCP/IP Gateways,"
PA Porras, A Valdes - Internet Society's Networks and Distributed ..., 1998 - vodun.org
... **Application-layer**-speci c sessions (eg, anonymous FT sessions pro led individually and/or collectively) ... Continuous measures are useful not only for **intrusion detection**, but also support the monitoring of health and status of the network from the perspective of connectiv- ity and ...
Cited by 15 - Related articles - View as HTML - All 13 versions

[PDF] **Intrusion** Prevention Systems (IPS): next generation firewalls
P Lindstrom - Spire Research Report, ozujak, 2004 - castle.eiu.edu
... In addition, the aberrations in communications protocols from network through **application layer** have no place in any sort of legitimate traffic, making the faults self-selective in a deterministic ... As long as there are packets on the network, there will be a need for **intrusion detection**. ...
Cited by 5 - View as HTML

Active trust management for autonomous adaptive survivable systems (atm's for aass's)
H Shrobe, J Doyle - Self-Adaptive Software, 2001 - Springer
... from a broad variety of sour- ces, including the application systems, **intrusion detection** systems, system ... illustrates that building a trust model involves more than just detecting an **intrusion**. ... These **application-layer** models are linked to models of the behavior of the computa- tional ...
Cited by 17 - Related articles - BL Direct - All 22 versions

Create email alert

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 Next

intrusion detection "application layer Search

Go to Google Home - About Google - About Google Scholar

Autograph: Toward automated, distributed worm **signature detection**
HA Kim, B Karp - Proceedings of the 13th conference on USENIX ..., 2004 - portal.acm.org
... labor, and thus significant delay: as network operators detect anomalous behavior, they communicate with one another and manually study packet traces to produce a worm **signature**. ... Network-Based **Application** Recognition. ... DShield - Distributed **Intrusion Detection** System. ...
Cited by 509 - Related articles - All 77 versions

[PDF] Snort-lightweight **intrusion detection** for networks
M Roesch - Proceedings of the 13th USENIX conference on ..., 1999 - usenix.org
... Page 6. Roesch Snort – Lightweight **Intrusion Detection** for Networks 4. itype: Match on the ICMP type field. ... The unique **signature** data in the **application** layer is the machine code just prior to the /bin/sh text string, as well as the string itself. ...
Cited by 1591 - Related articles - View as HTML - All 43 versions

A geometric framework for unsupervised anomaly **detection**: Detecting **intrusions** in unlabeled data
E Eskin, A Arnold, M Prerau, L Portnoy, S ... - Applications of Data ..., 2002 - Citeseer
... Abstract Most current **intrusion detection** systems employ **signature**-based methods or data mining ... 4, Data mining in work environments: Experiences in **intrusion detection** – Lee, Stolfo, et al. ... 4, Ecient clustering of high-dimensional data sets with **application** to reference matching ...
Cited by 424 - Related articles - Cached - All 5 versions

Service specific anomaly **detection** for network **intrusion detection**
C Krügel, T Toth, E Kirda - ... of the 2002 ACM symposium on Applied ..., 2002 - portal.acm.org
... The service independent part of the packet processing unit (PPU) has been realized with Snort [15]- Snort is an open- source, **signature** based network **intrusion detection** system that has the ability to reassemble ... The following two tables show the **application** model that ...
Cited by 215 - Related articles - All 12 versions

Intrusion detection for distributed **applications**
M Stillerman, C Marceau, M Stillman - Communications of the ACM, 1999 - portal.acm.org
... Ideally, all signatures of the running **application** under normal use are found in the self database ... With such coverage, it seems reasonable that the **signature** of cells during actual use will typically ... Note that if we run the **intrusion detection** system with a self database that does not ...
Cited by 74 - Related articles - BL Direct - All 6 versions

Intrusion detection techniques and approaches
T Verwoerd, R Hunt - Computer communications, 2002 - Elsevier
... In addition, attacks that use variations on the **signature** strings may bypass this type ... The simplest model of an IDS is a single **application**, containing probe, monitor, resolver ... themselves, suitable for feeding into a higher-level IDS structure, an **intrusion detection** hierarchy results. ...
Cited by 111 - Related articles - All 11 versions

Towards a taxonomy of **intrusion-detection** systems
H Debar, M Dacier, A Wespi - Computer Networks, 1999 - Elsevier
... less than 60 s. Reaching the final state s5 corresponds to a matched **signature**, and may ... A number of **applications** and network services use it, such as login, sendmail, nfs, **http** ... Therefore, a few **intrusion-detection** tools have been developed that use information provided by the ...
Cited by 419 - Related articles - All 19 versions

Honeycomb: creating **intrusion detection** signatures using honeypots
C Kreibich, J Crowcroft - ACM SIGCOMM Computer Communication ..., 2004 - portal.acm.org
... commonly asked questions are requests for signatures for a certain **application** or a ... provide a standalone applica- tion version of Honeycomb that performs **signature** generation on ... com/article/paxson98bro.html [2] M. Roesch, "Snort: Lightweight **Intrusion Detection** for Networks ...
Cited by 326 - Related articles - BL Direct - All 64 versions

Intrusion detection in wireless ad-hoc networks
Y Zhang, W Lee - Proceedings of the 6th annual international ..., 2000 - portal.acm.org
... For example, a **signature** rule for the "guessing password attack" can be "there are more than 4 failed login attempts within 2 min- utes". ... In the wireless networks, there are no firewalls to protect the services from attack. However, **intrusion detection** in the **application** layer is ...
Cited by 764 - Related articles - All 43 versions

Anomalous payload-based network **intrusion detection**
K Wang, SJ Stolfo - Recent Advances in **Intrusion Detection**, 2004 - Springer
... anomaly detector, rather than being depend- ent upon others deploying a specific **signature** for a ... first word or token of each input line out of the first 1000 **application** payloads, restricted ... The work of Kruegel et al [8] describes a service-specific **intrusion detection** sys- tem that is ...
Cited by 372 - Related articles - BL Direct - All 84 versions

Measuring normality in **HTTP** traffic for anomaly-based **intrusion detection**
JM Estévez-Tapiador, P García-Teodoro, JE Díaz- ... - Computer Networks, 2004 - Elsevier
... attack is described through the construction of a specific model, known as the attack "**signature**". ... **application** traffic, of interest concerning anomaly **detection**; (b) a new anomaly-based **intrusion detection** approach that uses knowledge related to the **application**-layer protocol ...
Cited by 35 - Related articles - All 6 versions

An **intrusion-detection** model
DE Denning - IEEE Transactions on software engineering, 1987 - ieeexplore.ieee.org
... pose **intrusion-detection** expert system, which we have called IDES. A more detailed description of the design and **application** of IDES is given in our final report [1]. The model has six main components: * Subjects: Initiators of activity on a target system- normally users. ...
Cited by 2110 - Related articles - All 32 versions

[PDF] NetSTAT: A network-based **intrusion detection** approach
G Vigna, RA Kemmerer - Computer Security **Applications** Conference, 1998 - Citeseer
... The type of **application** event determines the protocol used to interpret the stream. For example, the following **signature** action: [c.streamToServer [HTTPRequest r]]| r.method == "GET"; ... 2.3. Probes The probes are the active **intrusion detection** compo- nents. ...
Cited by 198 - Related articles - View as HTML - All 23 versions

Mimicry attacks on host-based **intrusion detection** systems
D Wagner, P Soto - Proceedings of the 9th ACM Conference on ..., 2002 - portal.acm.org
... expect that our techniques will apply more generally to host-based **intrusion detection** systems based ... remainder of this section de- scribes six simple ideas for avoiding **detection**, in order of ... to avoid causing any change whatsoever in the ob- servable behavior of the **application**. ...
Cited by 400 - Related articles - All 38 versions

Fusion of multiple classifiers for **intrusion detection** in computer networks
G Giacinto, F Roli, L Didaci - Pattern Recognition Letters, 2003 - Elsevier
... Columbia University and distributed as part of the UCI KDD Archive (**http**://kdd.ics **...** very similar feature values (ie, these feature values correspond to the **signature** of that **...** Therefore, in the context of **intrusion detection application**, the simple replication of patterns is a reasonable **...**
Cited by 105 - Related articles - All 14 versions

[PDF] **Application** of Neural Networks to **Intrusion Detection**
JP Planquart - SANS Institute, 2001 - Citeseer
... **Application** of Neural Networks to **Intrusion Detection ...** Approaches for the misuse **detection** model are : • expert systems, containing a set of rules that describe attacks • **signature** verification, where attack scenarios are translated into sequences of audit events • petri **...**
Cited by 23 - Related articles - View as HTML - All 7 versions

Intrusion detection: a brief history and overview
RA Kemmerer, G Vigna - Computer, 2002 - ieeexplore.ieee.org
... they model only known attacks, developers must regularly update their **signature** sets **...** Annual Computer Security **Application** Conference (ACSAC'98), IEEE CS Press, Los Alamitos, Calif **...** D. Curry and H. Debar, "**Intrusion Detection** Message Exchange For- mat: Extensible Markup **...**
Cited by 133 - Related articles - BL Direct - All 7 versions

Application intrusion detection using language library calls
AK Jones, Y Lin - **...** **Applications** Conference, 2001. ACSAC ..., 2001 - ieeexplore.ieee.org
... false **detection** or false alarm, occurs when a sequence generated by legitimate behavior is **...** an **intrusion** are detected as anomalous, ie, all sequences generated by the **intrusion** appear in **...** is difficult to collect **signature** sequences of all normal behavior for a complex **application**. **...**
Cited by 22 - Related articles - All 12 versions

Testing network-based **intrusion detection** signatures using mutant exploits
G Vigna, W Robertson, D Balzarotti - **...** of the 11th ACM conference on ..., 2004 - portal.acm.org
... One may argue that the **intrusion detection** system may be considered to be the test suite **...** historically ne- glecting to handle IPv6 traffic, allowing an attacker to evade **detection** by sending **...** are defined as mutations which occur at the session, presentation, and **application** layers of **...**
Cited by 120 - Related articles - All 27 versions

Learning rules for anomaly **detection** of hostile network traffic
MV Mahoney, PK Chan - **...** on Data Mining, 2003. ICDM 2003, 2003 - ieeexplore.ieee.org
... An important component of computer security is **intrusion detection**--knowing whether a system has **...** features such as addresses and port numbers, rather than **application** protocols **...** efficient, randomized algorithm called LERAD (Learning Rules for Anomaly **Detection**), which can **...**
Cited by 90 - Related articles - All 40 versions

Using decision trees to improve **signature**-based **intrusion detection**
C Kruegel, T Toth - Recent Advances in **Intrusion Detection**, 2003 - Springer
... mode) while host-based systems collect events at the operating system level, such as system calls, or at the **application** level. **...** This technique is utilized by the original version of Snort [14], arguably the most deployed **signature**-based network **intrusion detection** tool. **...**
Cited by 66 - Related articles - BL Direct - All 12 versions

[BOOK] **Intrusion detection** systems
R Bace, P Mell - 2001 - tricare.osd.mil
... Therefore, it is advisable to use an **Application**-based IDS in combination with Host-based and/or Network **...** to doing misuse **detection** (called "state-based" analysis techniques) that can leverage a single **signature** to detect **...** NIST Special Publication on **Intrusion Detection** Systems **...**
Cited by 252 - Related articles - View as HTML - BL Direct - All 129 versions

[PDF] Real time data mining-based **intrusion detection**
W Lee, S Hershkop, M Miller, W Fan, SJ Stolfo, PK ... - 2001 - Citeseer
... 7]. 3 Efficiency In typical **applications** of data mining to **intrusion** de- tection, **detection** models are produced off-line because the learning algorithms must process tremendous amounts of archived audit data. These **...**
Cited by 157 - Related articles - View as HTML - All 32 versions

Network **intrusion detection**
B Mukherjee, LT Heberlein, KN Levitt - IEEE network, 1994 - ieeexplore.ieee.org
... A SQL-based query language is pro- vided to allow the SSO the capability to design custom queries for **intrusion detection**. **...** Both run on IBM 3090s. Their goal is not to detect attacks on the operating system, but to detect abuses of the **application**, namely, the credit database. **...**
Cited by 696 - Related articles - BL Direct - All 10 versions

[PDF] A virtual machine introspection based architecture for **intrusion detection**
T Garfinkel, M Rosenblum - Proc. Network and Distributed Systems ..., 2003 - Citeseer
... that make fewer assumptions about memory structure (such as naive **signature** scans) as well **...** as attackers are increasingly masking their ac- tivities and subverting **intrusion detection** systems through tampering with the OS kernel [18], shared libraries, and **applications** that are **...**
Cited by 332 - Related articles - View as HTML - All 42 versions

[PDF] Immunity-based **intrusion detection** system: A general framework
D Dasgupta - Proceedings of 22nd National information Systems ..., 1999 - Citeseer
... Different functional modules of the **intrusion detection** system are shown in figure 2. In this figure **...** Figure 2. Different functional modules of the **detection** system. **...** multi-agent system will accommodate necessary agent interaction components and the **application** environment in an **...**
Cited by 165 - Related articles - View as HTML - All 23 versions

Learning fingerprints for a database **intrusion detection** system
S Lee, W Low, P Wong - Computer Security—ESORICS 2002, 2002 - Springer
... and Anomaly **Detection** Module **Signature** Database Database Server 3 4 Actions to be taken Database User 6 2 5 **Application** User 6 Transaction 1 **Application** Server Fig. 1. Architecture for DIDAFIT Page 6. Learning Fingerprints for a Database **Intrusion Detection** System 269 **...**
Cited by 77 - Related articles - BL Direct - All 5 versions

STATL: An attack language for state-based **intrusion detection**
ST Eckmann, G Vigna, RA Kemmerer - Journal of Computer Security, 2002 - IOS Press
... Page 9. ST Eckmann et al. / STATL: An attack language for state-based **intrusion detection** 79 an attack **signature** (eg, the value of a counter or the ownership of a file). **...** For example, an action may be the opening of a TCP connection or the execution of an **application**. **...**
Cited by 264 - Related articles - BL Direct - All 60 versions

[PDF] **Intrusion detection** systems: A survey and taxonomy
S Axelsson - 2000 - Citeseer
... These detectors will by their very nature resem- ble **signature** based systems since we still **...** The host based logs can include operating system kernel logs, **application** program logs, network **...** Security The ability to withstand hostile attack against the **intrusion detection** system itself **...**
Cited by 434 - Related articles - View as HTML - All 43 versions

Intrusion detection techniques for mobile wireless networks
Y Zhang, W Lee, YA Huang - Wireless Networks, 2003 - portal.acm.org
... system to match and identify known **intrusions**. For ex- ample, a **signature** rule for the "guessing password attack" can be "there are more than 4 failed login attempts within 2 minutes". **...** However, **intrusion detection** in the **application** layer is not only feasible, as discussed in **...**
Cited by 309 - Related articles - BL Direct - All 26 versions

A data mining framework for building **intrusion detection** models
W Lee, SJ Stolfo, KW Mok - sp, 1999 - computer.org
... An ideal **application** in **intrusion detection** will be to gather sufficient "normal" and "abnormal" audit ... 93% of the time, after two **http** connections with S0 flag are made to host ... We participated in the DARPA **Intrusion Detection** Eval- uation Program, prepared and managed by MIT ...
Cited by 524 - Related articles - BL Direct - All 113 versions

[PDF] An evaluation of negative selection in an artificial immune system for network **intrusion detection**
J Kim, PJ Bentley - Proceedings of GECCO, 2001 - Citeseer
... 4 NETWORK TRAFFIC DATA VS NETWORK **INTRUSION SIGNATURE** ... The port numbers of commonly used IP services, such as ftp, telnet, **http**, are fixed and belong to this ... One distinctive feature of a network **intrusion detection** problem is that the size of data, which defines "self ...
Cited by 189 - Related articles - View as HTML - All 30 versions

[PDF] A database of computer attacks for the evaluation of **intrusion detection** systems
K Kendall - 1999 - Citeseer
... which combines statistical anomaly **detection** from NIDES with **signature** verification. Specification-based **intrusion detection** [39] is a second approach that can be used to detect new attacks. It detects attacks that make improper use of system or **application** programs. ...
Cited by 232 - Related articles - View as HTML - All 27 versions

[PDF] A scalable clustering technique for **intrusion signature** recognition
N Ye, X Li - Proceedings of 2001 IEEE Workshop on Information ..., 2001 - Citeseer
... We develop the CCA-S algorithm to overcome these problems. The **application** of CCA to computer **intrusion detection** based on **signature** recognition demonstrates the better **detection** ... [2] Graham, R., FAQ: Network **Intrusion Detection** Systems, **http**://www.robertgraham ...
Cited by 34 - Related articles - View as HTML - All 7 versions

A revised taxonomy for **intrusion-detection** systems
H Debar, M Dacier, A Wespi - Annals of Telecommunications, 2000 - Springer
... is very focused, dependent on the operating system, version, platform, and **application**. ... In terms of techniques, knowledge-based **intrusion- detection** prototypes were first implemented using first ... Commercial products them mostly used a **signature** (ie pattern matching) approach. ...
Cited by 156 - Related articles - BL Direct - All 5 versions

Use of passive network mapping to enhance **signature** quality of misuse network **intrusion detection** systems
B Dayioglu, A Ozgit - ... of the Sixteenth International Symposium on ..., 2001 - Citeseer
... Citations. 551, Snort - Lightweight **Intrusion Detection** for Networks – Roesch - 1999. ... 57, Remote OS **Detection** Via TCP/IP Stack FingerPrinting – Fyodor - 1998. 36, Probing TCP implementations – Comer, Lin - 1994. ... 1, Transport and **Application** Protocol Scrubbing – al - 2000. ...
Cited by 16 - Related articles - Cached

Data mining aided **signature** discovery in network-based **intrusion detection** system
H Han, XL Lu, J Lu, C Bo, RL Yong - ACM SIGOPS Operating ..., 2002 - portal.acm.org
... The result is satisfactory for our **application**, since the traffic data size of attacking programs and ... Experiments show that it improves the efficiency and accuracy of **signature** discovery. ... State of the Practice of **Intrusion Detection** Technologies, page 38, **http**://www.sei.cmu.edu/pub ...
Cited by 25 - Related articles - BL Direct - All 3 versions

[PDF] Using genetic algorithm for network **intrusion detection**
W Li - Proceedings of the United States Department of Energy ..., 2004 - Citeseer
... The pattern/**signature** might be a static string or a set sequence of actions. ... 1999. "An **Application** of Machine Learning to Network **Intrusion Detection**." In Proceedings of 1999 Annual Computer

Security **Applications** Conf. (ACSAC), pp. 371-377. Phoenix, Arizona. **...**
Cited by 58 - Related articles - View as HTML - All 9 versions

The base-rate fallacy and the difficulty of **intrusion detection**
S Axelsson - ACM Transactions on Information and System Security ..., 2000 - portal.acm.org
... Signature-based **detection** systems promise to detect known attacks and violations easily codified into security policies in a timely and efficient manner. **...** Section 5 then continues with an **application** of the base-rate fallacy to the **intrusion detection** problem, given a set of **...**
Cited by 438 - Related articles - All 36 versions

Adaptive neuro-fuzzy **intrusion detection** systems
S Chavan, K Shah, N Dave, S Mukherjee, A Abraham, ... - 2004 - computer.org
... patterns from what it has learnt and acquired in the database but also with the **signature** database which **...** Biological Motivation, in Yamakawa T and Matsumoto G (Eds), Methodologies for the Conception, Design and **Application** of Soft **...** [8] KDD cup 99 **Intrusion detection** data set. **...**
Cited by 35 - Related articles - All 22 versions

An introduction to **intrusion detection**
A Sundaram - Crossroads, 1996 - portal.acm.org
... It can detect some attack signatures like the failed logins **signature** that the state transition model cannot do. **...** Dorothy Denning [3] introduced a Generic **Intrusion Detection** Model that was independent of any particular system, **application** environment, system vulnerability, or **...**
Cited by 175 - Related articles - All 33 versions

[PDF] Security in ad hoc networks: A general **intrusion detection** architecture enhancing trust b approaches
P Albers, O Camp, JM Percher, B Jouga, L Mé, ... - Proceedings of the 1st ..., 2002 - Citeseer
... The data to be analysed may be obtained on the host, in **application** or system **...** the network (for instance, by placing sniffers on interconnection equipment) by Network Based **Intrusion Detection** System (NIDS **...** Misuse **detection**, on the other hand, relies on the **signature** of attacks. **...**
Cited by 103 - Related articles - View as HTML - All 12 versions

[PDF] A software architecture to support misuse **intrusion detection**
S Kumar, EH Spafford - Proceedings of the 18th national information ..., 1995 - cs.rpi.edu
... This paper described a possible architecturefor structuring a misuse **intrusion** detector based on **...** as a library permits embedding this type ofmatching within **application** programs. **...** discuss computer security vulnerabilities, their exploitation and steps for prevention and **detection** . **...**
Cited by 183 - Related articles - View as HTML - All 8 versions

A framework for constructing features and models for **intrusion detection** systems
W Lee, SJ Stolfo - ACM Transactions on Information and System ..., 2000 - portal.acm.org
... For example, a **signature** rule for the "guessing password attack" can be "there are **...** Domain knowledge is used to determine the appropriate essential features for an **application**. **...** intrinsic" features are for general network analysis purposes, and not specific to **intrusion detection**. **...**
Cited by 513 - Related articles - All 64 versions

The 1999 DARPA off-line **intrusion detection** evaluation
R Lippmann, JW Haines, DJ Fried, J Korba, K Das - Computer Networks, 2000 - Elsevier
... Data collected to evaluate **intrusion detection** systems include network sniffing data from the inside and outside sniffers, Solaris Basic Security Module **...** of programmers, secretaries, managers and other types of users running common UNIX and Windows NT **application** programs **...**
Cited by 568 - Related articles - BL Direct - All 51 versions

Probabilistic techniques for **intrusion detection** based on computer audit data
N Ye, X Li, Q Chen, SM Emran, M ... - IEEE Transactions on ..., 2001 - ieeexplore.ieee.org

... and accurate in detecting known **intrusions**, but cannot detect novel **intrusions** whose **signature** patterns are ... that takes into account the or- dering property of multiple events for **intrusion detection**. The **application** of a Markov model helps answer the question about whether the ...
Cited by 151 - Related articles - BL Direct - All 7 versions

[PDF] Evaluating **intrusion detection** systems: The 1998 DARPA off-line **intrusion detection** evaluation
RP Lippmann, DJ Fried, I Graf, JW Haines, K ... - Proceedings of the ..., 2000 - Citeseer
... Participants ran their **intrusion detection** systems on this test data and returned a list of all attacks detected, without ... simulate hundreds of programmers, secretaries, managers, and other types of users running common UNIX **application** programs. ... **http** •smtp •pop3 •ftp •irc •telnet ...
Cited by 475 - Related articles - View as HTML - All 39 versions

[PDF] Fast content-based packet handling for **intrusion detection**
M Fisk, G Varghese - 2001 - Citeseer
... **Signature Detection** versus Packet Filtering: **Signature**-based **intrusion detection** systems such as the popular ... However, signa- ture **detection** systems go one step beyond packet filters in complexity by ... matching in packet content, is also of interest to many **applications** that make ...
Cited by 118 - Related articles - View as HTML - All 18 versions

A stateful **intrusion detection** system for world-wide Web servers
G Vigna, W Robertson, V Kher, RA ... - ... Security **Applications** ..., 2003 - ieeexplore.ieee.org
... domain-independent analysis engine that can be extended in a well-defined way to per- form **intrusion detection** analysis in specific **application** do- mains ... The STAT framework centers around an **intrusion** mod- eling technique that characterizes attacks in terms of transi- tions ...
Cited by 84 - Related articles - All 35 versions

[PDF] Fuzzy cognitive maps for decision support in an intelligent **intrusion detection** system
A Siraj, SM Bridges, RB Vaughn - IFSA World Congress and 20th NAFIPS ..., 2001 - Citeseer
... For certain types of attacks, the **signature** is either present or absent and the ... **Intrusion detection** systems.(**http**://www.cerias.purdue.edu/coast/c oast-library.html) [2 ... Genetic algorithms for feature selection in an **intrusion detection application** MS Thesis, Mississippi State University. ...
Cited by 61 - Related articles - View as HTML - All 6 versions

[PDF] The use of information retrieval techniques for **intrusion detection**
R Anderson, A Khattak - ... on the Recent Advances in **Intrusion Detection** (. . ., 1998 - Citeseer
... detecting attacks whose **signature** is an unusual combination of events, and they may consume only a very small additional amount of storage. This ap- proach allows the **intrusion detection** community to adopt a wide range of techniques developed in **applications** ranging from ...
Cited by 46 - Related articles - View as HTML - All 21 versions

Defending yourself: The role of **intrusion detection** systems
J McHugh, A Christie, J Allen - IEEE software, 2000 - ieeexplore.ieee.org
... Topics to consider include **detection** and response characteristics, use of **signature**- and anomaly-based ... to correlate alerts with other information such as system or **application** logs. ... The **Intrusion Detection** Working Group of the Internet Engineering Task Force is developing a ...
Cited by 155 - Related articles - BL Direct - All 35 versions

Alert correlation in a cooperative **intrusion detection** framework
F Cuppens, A Miege - 2002 - computer.org
... There are actually two main **intrusion detection** approaches: the behavioral approach (also called anomaly **detection**) and the **signature** analysis (also called misuse **detection**). Anomaly **detection** is based on statistical description of the normal behavior of users or **applications**. ...
Cited by 526 - Related articles - BL Direct - All 6 versions

Temporal signatures for **intrusion detection**
A Jones, S Li - ... **Applications** Conference, 2001. ACSAC 2001. ..., 2001 - ieeexplore.ieee.org
... It builds on an existing method of **application intrusion detection** developed at the University of New Mexico that uses a system call sequence as a **signature**. **...** Keywords: security, **application intrusion detection**, temporal **signature** 1. Introduction **...**
Cited by 26 - Related articles - All 15 versions

An anomaly **detection** technique based on a chi-square statistic for detecting **intrusions** into information systems
N Ye, Q Chen - Quality and Reliability Engineering ..., 2001 - interscience.wiley.com
... The limitation of **signature** recognition techniques can be overcome by using anomaly **detection** techniques **...** A report [20] on an **application** of the Hotelling's T 2 statistic to **intrusion ...** Proceed- ings of the 1st USENIX Workshop on **Intrusion Detection** and Network Monitoring, April **...**
Cited by 100 - Related articles - BL Direct - All 7 versions

[PDF] A pattern matching model for misuse **intrusion detection**
S Kumar, EH Spafford - ... of the 17th national computer security ..., 1994 - svn.assembla.com
... I n other cases the **signature** may specify arbitrary permutations of sub-patterns comprising the **...** A Pattern Matching ModeL For Misuse **Intrusion Detection ...** An **Application** ofPatternMatching in I ntrusionDetec- tion.TechnicalReport 94- 01 3 ,Purdue University,Department of **...**
Cited by 374 - Related articles - View as HTML - All 14 versions

Stateful **intrusion detection** for high-speed networks
C Kruegel, F Valeur, G Vigna, R Kemmerer - 2002 - computer.org
... packets from distributed denial-of-service slaves that produce traffic with a unique, known **signature**. **...** the same equipment as the traf- fic slicers), and they provide the **intrusion detection** sensors with a **...** and the correctly- ordered batch of packets is passed to the **application**, or the **...**
Cited by 223 - Related articles - BL Direct - All 41 versions

[PDF] Computer system **intrusion detection**: A survey
AK Jones, RS Sielken - ... of Virginia, Computer Science Department, Tech. ..., 1999 - Citeseer
... were large enough, the distributed Self-Nonself system could be constructed to ensure a unique Nonself **signature** for each node. **... Intrusion Detection ...** the entities monitored can also be workstations, network of workstations, remote hosts, groups of users, or **application** programs. **...**
Cited by 92 - Related articles - View as HTML - All 21 versions

Intrusion detection system: Technology and development
Y Bai, H Kobayashi - 2003 - computer.org
... [9] Tim Bass, "**Intrusion Detection** Systems and Multisensor Data Fusion", Communications of the ACM, April 2000/vol.43, No.4, pp99-105 [10] Steven Andrew Hofmeyr, An Immunological Model of Distributed **Detection** and Its **Application** to Computer Security, Ph.D **...**
Cited by 61 - Related articles - All 5 versions

Intrusion detection using sequences of system calls
SA Hofmeyr, S Forrest, A Somayaji - Journal of Computer Security, 1998 - IOS Press
... as sending or receiving mail), which require access to system objects that are not normally available to users or **application** programs. **...** processes also offers some advan- tages over monitoring user behavior, which is a more common approach to **intrusion detection** (for example **...**
Cited by 811 - Related articles - BL Direct - All 100 versions

[PDF] Evolving fuzzy classifiers for **intrusion detection**
J Gomez, D Dasgupta - Proceedings of the 2002 IEEE Workshop ..., 2002 - disi.unal.edu.co
... The main contribution of the present work is the design of a classification process for the **intrusion detection** problem. It allows **application** of fuzzy logic and genetic algorithms for the **detection** of various types of attacks. VI. ACKNOWLEDGES **...**

Cited by 112 - Related articles - View as HTML - All 17 versions

Designing and implementing a family of **intrusion detection** systems
G Vigna, F Valeur, RA Kemmerer - Proceedings of the 9th European ..., 2003 - portal.acm.org
... produced by the operating system auditing facilities, or log messages pro- duced by **applications**. ... community has developed a num- ber of different tools that perform **intrusion detection** in par ... In the specific case of **signature**-based **intrusion detection** systems [25, 18, 19, 11], the ...
Cited by 73 - Related articles - BL Direct - All 11 versions

[PDF] DIDS (distributed **intrusion detection** system)-motivation, architecture, and an early prot
SR Snapp, J Brentano, GV Dias, TL Goan, LT ... - Proceedings of the 14th ..., 1991 - Citeseer
... **Intrusion detection** systems designed for a network environment will become increasingly important as the ... We are designing a **signature** analysis component for the host monitor to detect ... purpose multi-user computers, we intend to develop monitors for **application** specific hosts ...
Cited by 324 - Related articles - View as HTML - All 18 versions

Stochastic protocol modeling for anomaly based network **intrusion detection**
JM Estevez-Tapiador, P Garcia-Teodoro ... - ... , 2003. IWIAS 2003. ..., 2003 - ieeexplore.ieee.org
... are well known and appropriate filters could be written and installed on a **signature** based IDS ... Figure 9 shows experimental **intrusion detection** results for this new model ... observed how the model detects protocol misuses similarly it was done by the **application**-dependant models ...
Cited by 21 - Related articles - All 9 versions

Intrusion and **intrusion detection**
J McHugh - International Journal of Information Security, 2001 - Springer
... The paper de- scribes the two primary **intrusion detection** techniques, anomaly **detection** and **signature**-based misuse ... Discovery represents the first **applications**-based IDS where **intrusions** against an **application** as opposed to a ... J. M c Hugh: **Intrusion** and **intrusion detection** 21 ...
Cited by 161 - Related articles - All 13 versions

Enhancing byte-level network **intrusion detection** signatures with context
R Sommer, V Paxson - Proceedings of the 10th ACM conference on ..., 2003 - portal.acm.org
... They con- tain misuse-**detection** components as well, but their signatures are defined at a higher ... to their general scope, both systems use a great deal of context to detect **intrusions**. ... Their expressiveness has made them a well-known tool in many **applications**, and their power ...
Cited by 154 - Related articles - All 32 versions

Sketch-based change **detection**: methods, evaluation, and **applications**
B Krishnamurthy, S Sen, Y Zhang, Y ... - Proceedings of the 3rd ..., 2003 - portal.acm.org
... network traffic is described in [9]. Methods for **intrusion** detec- tion include neural networks [20], Markov models [40], and ... where T is a parameter to be determined by the **application**. Now for any key a, the change **detection** module can reconstruct its forecast error in Se(t) using ...
Cited by 232 - Related articles - All 35 versions

Immune system approaches to **intrusion detection**–a review
U Aickelin, J Greensmith, J Twycross - Artificial Immune Systems, 2004 - Springer
... a number of dif- ferent research groups, with the common goal of implementing various AISs for **applications** within security ... viruses across networks, systems found to be infected contact neighbouring systems and transfer their **signature** databases to ... Network **Intrusion Detection**. ...
Cited by 125 - Related articles - BL Direct - All 22 versions

Generating realistic workloads for network **intrusion detection** systems
S Antonatos, KG Anagnostakis, EP ... - ACM SIGSOFT Software ..., 2004 - portal.acm.org
... The modules create **application**-specific traffic for protocols such as DNS, SMTP and HTTE and can be ... rate is the fraction of alarms that did not indi- cate a real **intrusion** over the total ... For a nIDS

that uses statistical anomaly **detection** methods, both metrics reflect the quality of the ...
Cited by 91 - Related articles - BL Direct - All 36 versions

NetSTAT: A network-based **intrusion detection** system
G Vigna, RA Kemmerer - Journal of Computer Security, 1999 - IOS Press
... For example, the **signature** action: ... The type of **application** event determines the protocol used to interpret the stream. For example, the following sig- nature action: ... Page 12. 48 G. Vigna and RA Kemmerer / NetSTAT: A network-based **intrusion detection** system 3.3. Probes ...
Cited by 228 - Related articles - BL Direct - All 4 versions

[PDF] An immunological model of distributed **detection** and its **application** to computer security
SA Hofmeyr, S Forrest - University of New Mexico, 1999 - Citeseer
... An Immunological Model of Distributed **Detection** and Its **Application** ... adapt to changing self sets; dynamic detectors to avoid consistent gaps in **detection** coverage; and memory, to implement **signature**-based **detection**. Thirdly, the model is applied to network **intrusion detection**. ...
Cited by 260 - Related articles - View as HTML - All 20 versions

A taxonomy for information security technologies
HS Venter, JHP Eloff - Computers & Security, 2003 - Elsevier
... Therefore, a VS is an information security technology which is but a special case of **intrusion detection** [17]. ... viruses and functions before they can cause havoc, much in the same way as VSs in that they also 'know' what a specific virus's **signature** looks like. ... At **application** level: A ...
Cited by 41 - Related articles - All 4 versions

[PDF] Global **intrusion detection** in the domino overlay system
V Yegneswaran, P Barford, S Jha - Proceedings of NDSS, 2004 - Citeseer
... node multicasts an **intrusion** summary, it first computes a SHA-1 hash of the summary and appends the digital **signature** of the ... information theoretic approach to quantify the additional information that is gained by adding new nodes in a distributed **intrusion detection** framework. ...
Cited by 205 - Related articles - View as HTML - All 24 versions

[PDF] An Achilles' heel in **signature**-based IDS: Squealing false positives in SNORT
S Patton, W Yurcik, D Doss - ... on Recent Advances in **Intrusion Detection** ..., 2001 - Citeseer
... We feel this is significant evidence to support the position that the major limitation of a **signature**-based IDS is not the ability to accurately detect misuse behavior but rather the ability to ... al., Building Adaptive and Agile **Applications** Using **Intrusion Detection** and Response. ...
Cited by 48 - Related articles - View as HTML - All 22 versions

Managing alerts in a multi-**intrusion detection** environment
F Cuppens - acsac, 2001 - computer.org
... functionality between different approaches, namely the behavioral and **signature** analysis approaches ... how we manage alert messages that come from different **intrusion detection** systems ... Proceedings of the 17th Annual Computer Security **Applications** Conference (ACSAC'01) 0 ...
Cited by 217 - Related articles - All 12 versions

[PDF] Computer **intrusion detection** through EWMA for autocorrelated and uncorrelated data
N Ye, S Vilbert, Q Chen - IEEE Transactions on Reliability, 2003 - Citeseer
... The **application** of the EWMA technique for uncorrelated data to **intrusion detection** takes the following 2 steps. ... [20] N. Ye, X. Li, and SM Emran, "Decision trees for **signature** recognition and state ... [21] N. Ye et al., "Probabilistic techniques for **intrusion detection** based on computer ...
Cited by 68 - Related articles - View as HTML - BL Direct - All 11 versions

Automated worm fingerprinting
S Singh, C Estan, G Varghese, S ... - Proceedings of the 6th ..., 2004 - portal.acm.org
... 1998. 30. [30] TH Ptacek and TN Newsham. Insertion, Evasion and Denial-of-Service: Eluding

Network **Intrusion Detection**. Technical report, Secure Networks Inc., Jan. 1998. **...** The EarlyBird System for Real-time **Detection** of Unknown Worms. **...** United States Patent **Application**. **...**
Cited by 466 - Related articles - All 93 versions

Improving **intrusion detection** performance using keyword selection and neural networks
RP Lippmann, RK Cunningham - Computer Networks, 2000 - Elsevier
... The network security monitor (NSM) was an early **signature**-based **intrusion detection** system that found **...** the development of public-domain software for pattern classification and the **application** of neural networks and statistics to problems in computer **intrusion detection**. **...**
Cited by 97 - Related articles - All 17 versions

On the **detection** of anomalous system call arguments
C Kruegel, D Mutz, F Valeur, G Vigna - Computer Security--ESORICS ..., 2003 - Springer
... is, they cannot detect **intrusions** for which they do not have a **signature**. Anomaly-based techniques [6,9,12] follow an approach that is complemen- tary to misuse **detection**. In their case, **detection** is based on models of normal behavior of users and **applications**, called 'profiles'. **...**
Cited by 121 - Related articles - BL Direct - All 32 versions

An experience developing an IDS stimulator for the black-box testing of network **intrusion detection** systems
D Mutz, G Vigna, R Kemmerer - 2003 - computer.org
... These mod- els may focus on the users, the **applications**, or the net- work. **...** The work presented in this paper proposes to use this attack technique as a means of generating test-cases for the black-box testing of **signature**-based **intrusion detection** systems. **...**
Cited by 52 - Related articles - All 18 versions

Anomaly **detection** of web-based attacks
C Kruegel, G Vigna - Proceedings of the 10th ACM conference on ..., 2003 - portal.acm.org
... anomaly de- tection systems tailored to detect attacks against web servers and web-based **applications**. **...** re- lated work on **detection** of web-based attacks and anomaly **detection** in general. **...** 3 describes an abstract model for the data analyzed by our **intrusion detection** system. **...**
Cited by 262 - Related articles - All 72 versions

[PDF] Attack languages
G Vigna, ST Eckmann, RA Kemmerer - Proceedings of the IEEE ..., 2000 - cert.org
... it should be possible to incorporate attack descriptions in an ID **application** for automatic **...** Design a **signature** that detects an attack composed of n events of a certain **... Intrusion Detection** Message Exchange Format: Extensible Markup Language (XML) Document Type Definition. **...**
Cited by 46 - Related articles - View as HTML - All 6 versions

Intrusion detection through learning behavior model
B Balajinath, SV Raghavan - Computer Communications, 2001 - Elsevier
... identify **intrusion** by searching for various **intrusion**/attack patterns (**signature**) which matches the **signature** stored in **...** behavior through machine learning techniques for **intrusion detection** are discussed in [1]. **Application** of genetic programming for **intrusion detection** in a **...**
Cited by 66 - Related articles - All 4 versions

NIST special publication on **intrusion detection** systems
R Bace, P Mell, BOOZ-ALLEN AND HAMILTON INC ... - 2001 - oai.dtic.mil
... and administrators are encouraged to address vulnerabilities (eg through public services such as ICAT, **http**://icat.nist.gov **...** can be drawn from different levels of the system, with network, host, and **application** monitoring most **...** Analysis – the part of **intrusion detection** systems that **...**
Cited by 31 - Related articles - View as HTML - All 2 versions

[PDF] Applying Mobile Agents to **Intrusion Detection** and Response.

WA Jansen, T Karygiannis, DG Marks - 2000 - Citeseer
... **intrusion detection** services within a single corporate information system, and a secure, integrated meta-learning system that combines the collective knowledge acquired by individual local agents. Data mining, like neural networks and other single-point learning **applications**, ...
Cited by 101 - Related articles - View as HTML - All 47 versions

Protocol analysis in **intrusion detection** using decision tree
T Abbes, A Bouhoula, M ... - ... Technology: Coding and ..., 2004 - ieeexplore.ieee.org
... Finally, as **application** layer protocols can be stacked one on the other, we define in each container the type and the address of the next container which will refer to the next stacked protocol. ... Using decision trees to improves **signature**-based **intrusion detection**. ...
Cited by 40 - Related articles - All 15 versions

[PDF] **Intrusion detection** with unlabeled data using clustering
L Portnoy, E Eskin, S Stolfo - ... of ACM CSS Workshop on Data ..., 2001 - freeworld.thc.org
... by the fact that in the P10 dataset more different types of **intrusions** were represented ... set than training on P3, which in turn manifested itself in the increased **detection** rate ... In an actual **application** of the system, the expected performance greatly depends on the composition of the ...
Cited by 440 - Related articles - View as HTML - All 36 versions

State transition analysis: A rule-based **intrusion detection** approach
K Ilgun, A Kemmerer, A Porras - IEEE transactions on software ..., 1995 - ieeexplore.ieee.org
... and Section 111-D concludes the discussion by presenting a functional description of STAT, which is a real-time **intrusion detection** tool. ... After the initial and compromised states of a penetration scenario have been identified, the key actions, called **signature** actions are identified ...
Cited by 543 - Related articles - BL Direct - All 29 versions

ADAM: a testbed for exploring the use of data mining in **intrusion detection**
D Barbará, J Couto, S Jajodia, N Wu - ACM SIGMOD Record, 2001 - portal.acm.org
... attacks that involved usually only one connection and that can be best identified by **signature**-based systems. ... NetStat: A Network-Based **Intrusion Detection** Approach. ... of the 1~t Annual Information Theory : 50 Years of Discovery Computer Security **Application** Conference, ...
Cited by 110 - Related articles - BL Direct - All 9 versions

Accurate, scalable in-network identification of p2p traffic using **application** signatures
S Sen, O Spatscheck, D Wang - Proceedings of the 13th ..., 2004 - portal.acm.org
... Sig- nature based traffic classification has been mainly performed in the context of network security such as **intrusion** and anomaly detec- tion (eg [5, 4, 19, 14]) where ... 5. **SIGNATURE** IMPLEMENTATION As stated earlier we concentrate on P2P **application detection** in TCP traffic ...
Cited by 434 - Related articles - All 28 versions

[PDF] **Intrusion detection**: A bioinformatics approach
S Coull, J Branch, B Szymanski, E Breimer - ... Security **Applications** ..., 2003 - Citeseer
... The novelty of our approach results from the **application** of techniques used in bioinformatics ... of commands produced by a potential intruder and the user **signature**, which is a ... test showed that the described algorithm yields a promising combination of **intrusion detection** rate and ...
Cited by 75 - Related articles - View as HTML - All 27 versions

[PDF] Towards an artificial immune system for network **intrusion detection**: An investigation of dynamic clonal selection
J Kim, PJ Bentley - Proceedings of the 2002 Congress on Evolutionary ..., 2002 - Citeseer
... human security officer acknowledges that this detector detects any **intrusion signature** (costimulation), the ... Its **Application** to Computer Security, PhD Thesis, Dept of Computer Science ... Bentley, P., (1999), "The Artificial Immune Model for Network **Intrusion Detection**, 7th European ...
Cited by 324 - Related articles - View as HTML - All 17 versions

Integrated access control and **intrusion detection** for web servers
T Ryutov, C Neuman, D Kim, L ... - IEEE transactions on ..., 2003 - ieeexplore.ieee.org
... 6.2 **Application**-Level **Intrusion Detection** We next **...** If the system identifiesrequestsfromanaddr essasmatchingknownattack **signature**, then subsequent requests from that host initiated by the same script, which checks for vulnerabilities not yet known, can still be blocked. **...**
Cited by 43 - Related articles - BL Direct - All 29 versions

[PDF] Minds-minnesota **intrusion detection** system
L Ertoz, E Eilertson, A Lazarevic, PN Tan, V ... - Next Generation Data ..., 2004 - Citeseer
... The network **intrusion** data con- tains several continuous attributes such as number of packets **...** In addition to the infor- mation reported by the anomaly **detection** module, the summarizer has **...** machine showed that it is also running multiple peer-to-peer file sharing **applications**. **...**
Cited by 106 - Related articles - View as HTML - All 11 versions

Intrusion detection in real-time database systems via time signatures
VCS Lee, JA Stankovic, SH Son - rtas, 2000 - computer.org
... For instance, **applications** that are responsible for reflecting the values of real world entities in **...** It provides a framework for a general-purpose **intrusion detection** expert system without focusing on a **...** that short sequences of system calls do provide a compact **signature** for normal **...**
Cited by 58 - Related articles - All 25 versions

[PS] A common **intrusion detection** framework
C Kahn, PA Porras, S Staniford-Chen, B ... - Submitted to Journal of ..., 1998 - Citeseer
... with the collection methods, analysis results, and response directives rarely intended to be shared across **intrusion detection** systems. While many techniques may, in principle, lend themselves to **applications** beyond their project objectives (eg, a **signature** analysis tool may **...**
Cited by 65 - Related articles - View as HTML - All 7 versions

Interfacing trusted **applications** with **intrusion detection** systems
M Welz, A Hutchison - Recent Advances in **Intrusion Detection**, 2001 - Springer
... may make it difficult to train an anomaly detector or specify a complete **signature**. **...** and that some attacks might be able to compromise a trusted **application** before it is **...** However, conventional **intrusion detection** systems are also fallible — the entire field of **intrusion detection** is a **...**
Cited by 20 - Related articles - BL Direct - All 8 versions

[PDF] A comparative analysis of current **intrusion detection** technologies
J Cannady, J Harrell - 4 th Technology for Information Security ..., 1996 - neurosecurity.com
... The concept involves the development of an electronic **signature** of a user based on their individual typing characteristics. **...** [1] NIDES is a real-time **intrusion detection application** which integrates a statistical analysis -based anomaly detector and a rule-based misuse **detection ...**
Cited by 35 - Related articles - View as HTML - All 4 versions

Signature-based methods for data streams
C Cortes, D Pregibon - Data Mining and Knowledge Discovery, 2001 - Springer
... with graphical models per se, and we encourage that com- munity to consider the **application** of their **...** called Hancock (Cortes, Fisher, Pregibon, Rogers and Smith, 2000) to support high-level programming of **signature**-based methods. **...** A survey of **intrusion detection** techniques. **...**
Cited by 49 - Related articles - BL Direct - All 12 versions

[PDF] Experiences with tripwire: Using integrity checkers for **intrusion detection**
GH Kim, EH Spafford - Systems Administration, Networking and Security ..., 1994 - Citeseer
... these changes to be noticed in a timely manner — a goal very similar to **intrusion detection**. Another **application** we note uses Tripwire to help salvage file systems not completely repaired by **...** be rebound to its original name by searching the database for a matching **signature**. **...**
Cited by 94 - Related articles - View as HTML - All 51 versions

Create email alert

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 Next

intrusion detection application signal Search

Testing network-based **intrusion detection** signatures using mutant exploits
G Vigna, W Robertson, D Balzarotti - ... of the 11th ACM conference on ..., 2004 - portal.acm.org
... One may argue that the **intrusion detection** system may be considered to be the test suite and **...** the procedure is costly enough that it is not per- formed for all **services** in typical **...** techniques are defined as mutations which occur at the session, presentation, and **application** layers of **...**
Cited by 120 - Related articles - All 27 versions

A comparative study of anomaly detection schemes in network **intrusion detection**
A Lazarevic, L Ertoz, V Kumar, A Ozgur, ... - Proceedings of the ..., 2003 - books.google.com
... Unlike **signature**- based **intrusion detection** systems, models of misuse are created automatically, and **...** data contains four main categories of attacks: • DoS (Denial of **Service**), for example **...** 98 evaluation represents a significant advance in the field of **intrusion detection**, there are **...**
Cited by 339 - Related articles - All 61 versions

[PDF] Data mining for network **intrusion detection**
P Dokas, L Ertoz, V Kumar, A Lazarevic, J ... - Proc. NSF Workshop on ..., 2002 - Citeseer
... Unlike **signature**-based **intrusion detection** sys- tems, models of misuse are created **...** first applied the proposed **intrusion detection** schemes to 1998 DARPA **Intrusion Detection** Evaluation Data [9 **...** data contains four main categories of attacks: • DoS (Denial of **Service**), for example **...**
Cited by 107 - Related articles - View as HTML - All 9 versions

[PDF] Experiences with tripwire: Using integrity checkers for **intrusion detection**
GH Kim, EH Spafford - Systems Administration, Networking and Security ..., 1994 - Citeseer
... U NIX style pipes also allows for outside programs to supply encryption and compression **services** — ser- vices **...** to system admin- istrators was one of the goals of writing Tripwire, the variety of **applications** of Tripwire outside the do- main of **intrusion detection** has been **...**
Cited by 94 - Related articles - View as HTML - All 51 versions

[PDF] Minds-minnesota **intrusion detection** system
L Ertoz, E Eilertson, A Lazarevic, PN Tan, V ... - Next Generation Data ..., 2004 - Citeseer
... The Minnesota **Intrusion Detection** System (MINDS) is a data mining based system for detecting network **...** For example, scanning activity for a particular **service** can be summarized by a frequent set **...** showed that it is also running multiple peer-to-peer file sharing **applications**. **...**
Cited by 106 - Related articles - View as HTML - All 11 versions

[PDF] Detection of novel network attacks using data mining
L Ertoz, E Eilertson, A Lazarevic, PN Tan, P ... - Proc. of Workshop on ..., 2003 - Citeseer
... Policy violations. MINDS anomaly detection module is much more successful than SNORT in detecting policy violations (eg rogue and unauthorized **services**), since it looks for unusual network behavior **...** A number of **applications** outside of **intrusion detection** have similar **...**
Cited by 30 - Related articles - View as HTML - All 6 versions

M-commerce security: the impact of wireless **application** protocol (WAP) security **services** on

business and e-health solutions
J Tan, HJ Wen, T Gyires - International Journal of Mobile ..., 2003 - inderscience
... Authentication protocols and **intrusion detection** are also being put in place and sophisticated forms of ... With a proper **application**, mobile devices can also offer solutions to billing, prescriptions ... Real-time wireless e-health information **services** (eg a redesign and modification of e ...
Cited by 19 - Related articles - All 7 versions

Decentralized trust management and accountability in federated systems
BN Chun, A Bavier - Proceedings of the 37th Annual Hawaii ..., 2004 - ieeexplore.ieee.org
... In traditional net- work **intrusion detection** systems (NIDS) [3,18,21,24], incoming network traffic is scrutinized and rules are ap ... scrutinize outgoing network traffic and to generate warnings (and take actions, such as suspending the offending **application** of **service**) on potentially ...
Cited by 19 - Related articles - All 14 versions

[PDF] Detection and summarization of novel network attacks using data mining
L Ertoz, E Eilertson, A Lazarevic, P Tan, P ... - ... **INtrusion Detection** ..., 2003 - Citeseer
... Unlike **signature**-based **intrusion detection** systems, models of misuse are created automatically, and can ... The Minnesota **Intrusion Detection** System (MINDS) is a data mining based system for detecting network ... in the last T seconds, since typically of Denial of **Service** (DoS) and ...
Cited by 26 - Related articles - View as HTML - All 9 versions

Bro: a system for detecting network intruders in real-time* 1
V Paxson - Computer networks, 1999 - Elsevier
... Because **intrusion detection** can form a cornerstone of the security measures available to a ... Depending on how it is written, the FTP **application** receiving this text might ... UDP definitions, but, more fundamentally, erodes portability because a getservbyname **service** name known ...
Cited by 1421 - Related articles - All 170 versions

Web tap: detecting covert web traffic
K Borders, A Prakash - Proceedings of the 11th ACM conference on ..., 2004 - portal.acm.org
... Markov chains or other models has been used for host and network **intrusion detection** [9, 15 ... difficult to collect enough data to do probabilistic analysis for every web **application** to build ... for allowing legitimate users to bypass firewalls and get access to remote **services**, they can ...
Cited by 64 - Related articles - All 19 versions

[DOC] Auralization of **intrusion detection** system using Jlisten
MC Gopinath - Development, 2004 - cs.purdue.edu
... packet; TCP packet with SYN&FIN flag set; Detection of denial of **Service** attacks; Detection ... In Proceedings of the 19th Annual International Computer Software and **Applications** Conference (COMPSAC ... [3] Martin Roesch et.al, "Snort, A lightweight **Intrusion Detection** System", **http** ...
Cited by 4 - Related articles - View as HTML - All 2 versions

[PDF] Protecting against cyber threats in networked information systems
L Ertoz, A Lazarevic, E Eilertson, PN Tan, P Dokas, ... - Proceedings of ..., 2003 - Citeseer
... applicable provided labeled training data (normal and abnormal users' or **applications**' behavior) are ... Anomaly Detection Anomaly detection is a key element of **intrusion detection** in which ... than SNORT in detecting policy violations (eg rogue and unauthorized **services**), since it ...
Cited by 14 - Related articles - View as HTML - All 10 versions

[PDF] Yalta: A secure collaborative space for dynamic coalitions
GT Byrd, F Gong, C Sargor, TJ Smith - ... of the 2001 IEEE Workshop on ..., 2001 - Citeseer
... LDAP Database **Intrusion Detection** System Private Key Share Servers Fig. ... 7 vices will be tested by having several mock **applications** invoking such **services** with each other. This experiment will be conducted independently on both the testbeds at MCNC and NCSU. ...
Cited by 21 - Related articles - View as HTML - All 7 versions

[PDF] An Active Network **Services** Architecture for Routers with Silicon-Based Forwarding Engi
R Jaeger, R Duncan, F Travostino, T Lavian, J ... - Proceedings of ..., 1999 - Citeseer
... acts as a server for all control plane needs (see Figure 3); - **Intrusion detection**: By correlating **...** JFWD discloses a more privileged perspective on system behaviors than management **applications** would get **...** Specifically, the ORE **services** can use the JFWD API to request receipt **...**
Cited by 4 - Related articles - View as HTML - All 5 versions

[PDF] Passive Vulnerability Detection
R Gula - Network Security Wizards, 1999 - vodun.org
... For **intrusion detection** and network forensics, this is very important. **...** If Telnet is in use on a given network, then a **signature** like this may be worth looking for. **...** Other examples of configuration problems may include inbound access to sensitive **services**. Consider Page 3 of 5 **...**
Cited by 2 - Related articles - View as HTML - All 2 versions

[HTML] Cost effective security for small businesses
SR Brown - Proceedings of the FREENIX Track: 2001 USENIX ..., 2001 - usenix.org
... The goal is to detect specific traffic based on a given **signature** and then optionally taking some type of action. **...** Table 2.8 - Network **Intrusion Detection**. **...** The FWTK also supports proxies for a number of other **application services** such as FTP, **HTTP**, X server, Telnet, and SMTP. **...**
Cited by 1 - Related articles - Cached - All 3 versions

A framework for classifying denial of **service** attacks
A Hussain, J Heidemann, C ... - ... on Applications, ..., 2003 - portal.acm.org
... an ongoing attack using either anomaly-detection [13, 25, 38] or **signature**-scan techniques **...** to exercise specific soft- ware bugs within the target's OS or **application**, disabling the **...** secured hosts, reflectors are typically legitimate hosts providing Internet **services**, making reflector **...**
Cited by 330 - Related articles - BL Direct - All 62 versions

[CITATION] The PF_CINIC Protocol Family Interface
E Hawkins - 2003 - California Polytechnic State ...
Related articles - All 2 versions

[PDF] Reclaiming one's bandwidth: Dynamic filtering of traffic based on packet payload content
B Irwin - 2000 - Citeseer
... and filtering of these traffic types can be implemented with methods commonly used by **Intrusion Detection** Systems (IDS **...** level rather than having rules dynamically generated, yet the dynamic generation will still catch **services** running on other **...** 'Port hopping' **applications** such as **...**
Related articles - View as HTML - All 3 versions

A comparative experimental evaluation study of **intrusion detection** system performance in a gigabit environment
C Iheagwara, A Blyth, M Singhal - Journal of Computer Security, 2003 - IOS Press
... with valid headers and checksums so that the switches would never pass them to the **intrusion detection** system (IDS **...** suite or created an interactive TCL and Casl scripts to log into the appropriate **service** to run **...** Each **signature** was set to count the number of packets it triggers. **...**
Cited by 12 - Related articles - BL Direct - All 5 versions

A machine learning approach for efficient traffic classification
W Li, AW Moore - mascots, 1899 - computer.org
... **Intrusion detection** systems would ideally require zero false-negative rate and low-latency identification **...** 0.0 Peer-2-Peer 92.5035 96.0884 Database 96.7181 19.2249 **Service** 99.6323 97.5696 **...** ability of han- dling encrypted traffic and previously unknown **applications**, based on **...**
Cited by 12 - Related articles - All 10 versions

[PDF] Extending **Intrusion Detection** with Alert Correlation and Intrusion Tolerance

D Gorton - Licentiate thesis, Chalmers University of Technology, 2003 - cs.uccs.edu
... The purpose of access control is to restrict access to objects or **services** to only authorized users. The purpose of non-repudia- tion is to provide proof of delivery and sender identity. ... [100]. **Intrusion Detection** System Behavior on detection ... Network packets **Application** logfiles ...
Cited by 7 - Related articles - View as HTML - All 6 versions

[PDF] A worst-case worm
N Weaver, V Paxson, S Staniford - Proc. Third Annual Workshop on ..., 2004 - Citeseer
... of the worm to elude the market- leading anti-virus and **intrusion detection** systems on ... to restore the system: reload the op- erating system, install patches, reinstall **applications**, re- store ... Some institutions use remote install techniques or similar **services** but, even then, significant ...
Cited by 54 - Related articles - View as HTML - All 34 versions

[PDF] Configurable Middleware-level **Intrusion Detection** Support for Embedded Systems
E NÆSS - 2004 - research.wsuibs.wsu.edu
... Interval Procedural Misuse Responses EMIDS Middleware Logic Networking API and Other OS **Services application**-based **intrusion detection** system based on anomaly and misuse detection. **Application** Layer Middleware Layer Operating System Layer IDS kernel ...
Cited by 2 - Related articles - View as HTML - All 5 versions

[PDF] Passive network discovery for real time situation awareness
A De Montigny-Leboeuf, F Massicotte - 2004 - Citeseer
... Traditional network security devices such as **Intrusion Detection** Systems (IDS), firewalls, and security scanners operate ... Determining what **services** a machine provides can help network administrators identify prohibited or potentially vulnerable network **applications**. ...
Cited by 14 - Related articles - View as HTML - All 14 versions

[PDF] A Unified Patch Management Architecture
D White, B Irwin - ... Telecommunication Networks and Application ..., 2004 - satnac.org.za
... D. Fetching Patches Currently, system and **application** patches are distributed over various media and the ... vulnerable and is often in a situation where it cannot turn off a critical **service**. ... related patches can be can be used in conjunction with an **Intrusion Detection** System (IDS ...
Cited by 1 - Related articles - View as HTML - All 2 versions

[PDF] **Intrusion Detection** and the Use of Deception Systems
S Rajan, T San Marcos - Theses and Dissertations- ..., 2003 - ecommons.txstate.edu
... issues when developing these **applications**. 2.2.2. Portscans ... 2.5.1. Issues with Network **Intrusion Detection** o Speed of Data Processing ... packets since they are usually used in denial of **service** attacks. There are many programs that generate large packets naturally. ...
Related articles - All 6 versions

Behavioral authentication of server flows
JP Early, CE Brodley, C Rosenberg - 2003 - computer.org
... As stated previously, in the presence of a proxy or compromised **service**, this system ... These classifiers can augment tradi- tional **intrusion detection** systems to detect artifacts of suc ... Proceedings of the 19th Annual Computer Security **Applications** Conference (ACSAC 2003) 1063 ...
Cited by 45 - Related articles - All 17 versions

Defense Information Warfare Technology **Applications** (DIWTA) Automated **Intrusion Detecti** Environment (AIDE) Advanced Concept Technology Demonstration (...
P Danno, NORTHROP GRUMMAN INFORMATION ... - 2004 - oai.dtic.mil
... suggestions for reducing this burden to Washington Headquarters **Services**, Directorate for ... 4. TITLE AND SUBTITLE DEFENSE INFORMATION WARFARE TECHNOLOGY **APPLICATIONS** (DIWTA) (AUTOMATED **INTRUSION DETECTION** ENVIRONMENT (AIDE ...
View as HTML - All 2 versions

[PDF] Traffic Analysis: from Stateful Firewall to Network **Intrusion Detection** System
F Guo, T Chiueh - RPE Report, January, 2004 - Citeseer
... Network **Intrusion Detection** Systems (NIDS ... Otherwise, some nodes may not be able to **service** the request blindly dispatched from the layer-4 switch if they don't ... Normally the NIDS has a set of signatures which have to show up in the **application** layer byte stream of the packets ...
Cited by 4 - Related articles - View as HTML - All 5 versions

Dynamic Virtual LANs for Adaptive Network Security
D Merani, A Berni, M Leonard, NATO UNDERSEA ... - 2004 - oai.dtic.mil
... The segmentation of the network, combined with **intrusion detection** performed on the local traffic, gives the ... VLANs provide not only better quality of **service** to different workgroups, but also allow the quick ... [2] Leonard, M., Berni, A., Merani, D., "INSC **applications** for undersea ...
Related articles - View as HTML - All 5 versions

TCP/IP security threats and attack methods
B Harris, R Hunt - Computer Communications, 1999 - Elsevier
... Other preventative methods require changes to the network aspects of the operating system, or the addition of **intrusion detection** tools. ... 3. Threats to standard TCP/IP **services**. TCP/IP supports the operation of a number of well known **services** (ie **applications**). ...
Cited by 81 - Related articles - All 6 versions

Integrating software lifecycle process standards with security engineering
Y Lee, J Lee, Z Lee - Computers & Security, 2002 - Elsevier
... or firmware such as crypto systems, digital **signature**, firewall, **intrusion detection** systems and ... Therefore, information on security **services** and mechanisms will help us enhance our ... Engineering," Proceedings of the 10th Annual Computer Security **Applications** Conference, pp. ...
Cited by 19 - Related articles - All 3 versions

[PDF] Candid Wüest Desktop Firewalls and **Intrusion Detection**
D Zamboni, M Rennhard, B Plattner - 2002 - tik.ee.ethz.ch
... to include features to report known attacks that have been detected, similar to **intrusion detection** systems. ... Both are often used in denial of **service** or nuke attacks, which try to crash the ... can lead to problems if we want to have **non-standard** rules for standard **applications** like web ...
Related articles - View as HTML - All 5 versions

[PDF] Event-based document sensing for insider threats
K Anderson, A Carzaniga, D Heimbigner, A ... - University of Colorado, ..., 2004 - Citeseer
... In a content-based **service** model, message content is structured as a set of ... Again we are drawing on **intrusion detection** systems which first defined the notion of **signature**. ... to dynamically modify the operation and existence of sensors in integrated **applications** and operating ...
Cited by 5 - Related articles - View as HTML - All 7 versions

Using root cause analysis to handle **intrusion detection** alarms
K Julisch - 2003 - eldorado.tu-dortmund.de
... Sections 2.3.3 and 2.3.4 summarize other, less closely related **applications** of data ... However, some IDSs trigger alarms when they observe unknown protocols or ex- ploitable **services**. ... it is typical of the kind of assumptions made in **signature**-based **intrusion detection** and, more ...
Cited by 35 - Related articles - Cached - All 6 versions

Peer-to-Peer workload characterization: techniques and open issues
M Andreolini, M Colajanni, R ... - ... on Hot Topics in Peer-to- ..., 2004 - ieeexplore.ieee.org
... The file shar- ing **application** inherits from peer-to-peer systems two main characteristics, that is ... Both them are key characteristics for the de- ployment of a world-wide **service** such as ... A typical issue of **Intrusion Detection** System, where complex matching has to be carried out on ...
Cited by 3 - Related articles - All 6 versions

Private authentication
M Abadi - Proceedings of the 2nd international conference on ..., 2002 - portal.acm.org
... This examination may be costly, perhaps opening the door to a denial-of-**service** attack against B. In other situations, A might have included the name B, the key KB, or ... Protocols us- ing anonymous connections: Mobile **applications**. ... **Intrusion detection** in wireless ad-hoc networks ...
Cited by 95 - Related articles - BL Direct - All 23 versions

[CITATION] Socket API Extensions to Extract Packet Header Information List (PHIL)
R Narayan - 1999
Cited by 3 - Related articles - All 3 versions

[PDF] Engineering Issues for an Adaptive Defense Network
A Plaszcz, N Orlans, Z Eyler-Walker, D Moore - 2001 - Citeseer
... Achieving network defense in the future will involve: coordination between **service** providers, **intrusion detection**, auditing, ... It provides high-quality network **service** by controlling the bandwidth assigned to **applications** and users, prioritizing traffic, and building ...
Cited by 2 - Related articles - View as HTML - All 13 versions

[PDF] Open-Source Security Testing Methodology Manual
C VERSION - 2000 - Citeseer
... www.opst.org - www.opsa.org 9. **Intrusion Detection** System Testing ... 98 Denial of **Service** Template ... In the 2.5 revision of the OSSTMM we have evolved the definition and **application** of RAVs to more accurately quantify this risk level. ...
View as HTML - All 6 versions

[PDF] Detecting Signs of Intrusion
J Allen, E Stoner, CARNEGIE-MELLON UNIV ... - 2000 - dtic.mil
... 1-2 and the accompanying description in State of the Practice of **Intrusion Detection** Technologies [Allen ... establishing initial configurations of **applications**, operating systems ... the process of detecting signs of intrusion • using security monitoring and reporting **services** provided by ...
All 4 versions

Funkspiel schemes: An alternative to conventional tamper resistance
J Hastad, J Jonsson, A Juels, M Yung - Proceedings of the 7th ACM ..., 2000 - portal.acm.org
... In this scheme, the sender updates her secret key through **application** of a suitable pseudorandom generator . ... funkspiel schemes as described above are vulnerable to a form of denial-of- **service** attack ... When such an outer MAC or **signature** is applied, the inner MAC used in the ...
Cited by 14 - Related articles - All 6 versions

Engineering Issues for an Adaptive Defense Network
D Moore, A Plaszcz, N Orlans, Z Eyler-Walker - 2001 - Storming Media
... Achieving network defense in the future will involve: coordination between **service** providers, **intrusion detection**, auditing, automated ... tools coordinate various network related abuse as described in Appendix A to deny **service** to the target(s). Attack **applications** are maturing ...

Distinguishing between single and multi-source attacks using signal processing* 1
A Hussain, J Heidemann, C Papadopoulos - Computer Networks, 2004 - Elsevier
... Research on denial of **service** attacks is primarily focused on attack detection and response mechanisms. ... Bro, an **intrusion detection** system uses change in (statistical) normal behavior of **applications** and protocols to detect attacks [29] while Cheng use spectral ...
Cited by 8 - Related articles - All 13 versions

Dynamic and risk-aware network access management
L Teo, GJ Ahn, Y Zheng - ... of the eighth ACM symposium on Access ..., 2003 - portal.acm.org
... we aim to design a new approach to complement existing firewalls and **intrusion detection** systems ...

In order to cater for distributed and multi-tiered **applications**, access control has to be per ... can bypass firewalls by posing as legitimate traffic are rogue web **services** and malformed **...**
Cited by 18 - Related articles - All 5 versions

The Self-diagnosing **Intrusion Detection** System Mechanism
CT Yang - 2004 - etdncku.lib.ncku.edu.tw
... In the meantime, the risk of unauthorized access and destruction of **service** by outsiders is increasing. **...** System (CMDS) [34] by Science **Applications** International Corporation. The drawback of the centralized approach to **intrusion detection** was that it introduces a single point of **...**
Related articles - All 2 versions

[PDF] An intrusion tolerance approach for protecting network infrastructures
S Cheung - 1999 - Citeseer
... municate with it. In other words, DNS attacks can cause denial of **service**. As another **...** as if they were genuine. Some **applications** (eg, Unix rlogin) use name-based authenti- cation. **...** ing properties of the solutions. Most of the existing **intrusion detection** works are **...**
Cited by 12 - Related articles - View as HTML - All 7 versions

[BOOK] Maximum wireless security
C Peikari, S Fogie - 2003 - books.google.com
... Attacks 287 Server Attacks 287 Deploying VPNs in WLANs 288 Summary 290 14 **Intrusion Detection** Systems 291 **...** Publisher Sams Publishing 800 East 96th Street Indianapolis, IN 46240 USA Reader **Services** For more **...** Maximum Wireless Security and real-world **applications**. **...**
Cited by 36 - Related articles - Library Search - All 3 versions

[PDF] Distributed measurements on packet streams in the Internet
E Klaveness, KA Bakke - 2004 - domen.uninett.no
... **HTTP** Hypertext Transfer Protocol **...** The traditional Internet is changing from being an unreliable, best-effort, packet deliv- ery **service** to becoming a multi-**service** network that supports **applications** with the need for end-to-end performance guarantees. **...**
Related articles - View as HTML

Applying Security Patches
BOOZ-ALLEN AND HAMILTON INC MCLEAN VA - 2001 - oai.dtic.mil
... This software is often called a patch, hotfix, or **service** pack. **...** During June 2001, a network security company discovered a serious vulnerability in Microsoft IIS web server **application**. **...** CERT 2 (**http**://www.cert.org) estimates that 95 percent of all network intrusions could be avoided **...**
View as HTML

[PDF] Secure execution environment for Java electronic **services**
A Herzog - 2002 - Citeseer
... Is the described secure execution environment suitable for use in an **application** server (residential gateway) running e-**services** in a home environment? **...** It is a Java **application** that can run other Java **applications**, namely e-**services**. **...**
Cited by 4 - Related articles - View as HTML - All 5 versions

[PDF] Network Survivability Analysis of the Navy and Marine Corps Intranet (NMCI)
AB Fahrenthold, NAVAL POSTGRADUATE SCHOOL . . . - 2002 - dtic.mil
... 115 B. NMCI SECURITY STRATEGY .....120 C. INITIATIVE CEDED TO THE ATTACKER .....124 1. **Intrusion Detection** Systems .....125 2 **... application** of network survivability to NMCI relevant. **...** network is its capability to provide essential **services** in **...**
View as HTML - All 7 versions

[BOOK] Active networks and active network management: a proactive management framework
SF Bush, AB Kulkarni - 2001 - books.google.com

... when installed at the active nodes, modifies their behavior to suit **application** requirements. ... A box template describes the input/output port **signature** and the internal topological ... Each switchlet provides **services** in the form of methods manipulating protocols implemented for that ...
Cited by 55 - Related articles - All 4 versions

[PDF] Feasibility Study on the Use of the ASP Business Model for Enterprise **Application** Softw
S Voß, DWIT Reiners, JR Beer, T Falkowski - 2002 - mmlab.ceid.upatras.gr
... The provision of **application services** invokes several technical requirements. ... "An **Application Service** Provider, or ASP, is any company that delivers and man- ages **applications** and computer **services** to subscribers/clients remotely via the Internet or a private network." ...
Related articles - View as HTML - All 2 versions

Network **Service** Misuse Detection: A Data Mining Approach
H Hsiao - 2004 - etd.lib.nsysu.edu.tw
... subsequently detecting possible backdoors. Moreover, several open-source network management tools (eg, SNORT1 for network **intrusion detection**) analyze packet ... commerce **applications**. ... reflecting use of particular protocols, thereby identifying the types of network **services**. ...
Related articles - All 2 versions

[PDF] NetSPA: a network security planning architecture
ML Artz - 2002 - mit.dspace.org
... In addition, expert attackers tend to go through many actions to both limit visibility to **intrusion detection** systems and quickly exploit targets. ... in the future. Such "leave behinds" might be Trojan software, network sniffers, or additional back-door network **services**. Cleanup. ...
Cited by 26 - Related articles - All 3 versions

[PS] Efficient threshold cryptosystems
S law Jarecki - 2001 - Citeseer
... Sensitive secret-key decryption **services** could also be subject to such attacks. ... The servers that participate in a threshold scheme should be additionally protected with **intrusion-detection** software, firewalls, back-ups, and physical ... **APPLICATIONS** OF THRESHOLD SCHEMES ...
Cited by 19 - Related articles - View as HTML - All 5 versions

[PDF] How to Crack WEP or Bluetooth Without Sniffing a Single Packet OR
B Guessing, J Searches - 2004 - leetupload.com
... Example: Sending a Packet of Data .....49 (7) **Application** Layer (SMTP, **HTTP**, FTP, telnet ... 85 Operating System.....85 Protocols/**Services**/**Applications** .....85 Exploit ...
Related articles - View as HTML

Comparative Analysis of Active and Passive Mapping Techniques in an Internet-Based Local A Network
JB Kuntzelman, AIR FORCE INST OF TECH WRIGHT- ... - 2004 - oai.dtic.mil
... Ports 1-1024 are reserved for well-known **services**. For instance, the Simple Mail Transfer Protocol (SMTP), the de-facto standard for passing electronic mail, is typically found at port 25 and Hy- pertext Transfer Protocol (**HTTP**, the protocol of the world-wide web), is typically ...
Cited by 4 - Related articles - View as HTML - All 3 versions

[PDF] Access Control for Ad-hoc Collaboration
D Balfanz, EW Felten - Princeton University, Princeton, NJ, 2001 - cs.princeton.edu
... 2 real-time systems, **intrusion-detection** mechanisms, and others, failed to have an impact on the personal computer. ... Distributed Java **Applications** 1 ... every new client needs to be introduced to the server before it can start using the **service**. Ad-hoc collaboration is impossible. ...
Cited by 16 - Related articles - View as HTML - All 3 versions

[BOOK] Inside Windows 2000 Server

W Boswell - 2000 - books.google.com
... 955-6 Domino System Administration Rob Kirkland ISBN: 1-56205-948-3 Cisco Router Configuration & Troubleshooting Mark Tripod ISBN: 0-7357-0024-9 Network **Intrusion Detection**: An Analyst's ... Intended for file-and-print **services** and general-purpose **applications**. ...
Cited by 6 - Related articles - Library Search - All 2 versions

[**BOOK**] Integrating Linux and Windows
M McCune - 2001 - books.google.com
... 180 17.4.8 Running Other **Services** over SSH . . . ... Windows is king of the desktop for good reason. It has a polished interface and more end-user **applications** than any other operating system. It is also pre-installed on most new PCs, making it an easy, safe choice for most PCs. ...
Cited by 2 - Related articles - All 4 versions

[**PDF**] Modulo 7
SA Informatica, I Tecnologica - 2003 - 212.189.172.195
... Microsoft Windows 2000 Advanced Server è la piattaforma software raccomandata per **application** server dipartimentali che necessitano ... oltre a consentire l'accesso a fileserver Novell, offre funzionalità di NetWare Directory **Service** (NDS). ... **http**://thehamptons.com/anders/netatalk ...
View as HTML - All 12 versions

[**PDF**] Modulo 7
RDG per i Sistemi - 2003 - itisondrio.it
... 2000 Advanced Server è la piattaforma software raccomandata per **application** server dipartimentali ... l'accesso a fileserver Novell, offre funzionalità di NetWare Directory **Service** (NDS). ... di rete (configurazione, analisi del traffico, ...) e della sicurezza in rete (**intrusion detection**, ...) ...
Related articles - View as HTML

 Create email alert

Intrusion detection system for high-speed network
W Yang, BX Fang, B Liu, HL Zhang - Computer Communications, 2004 - Elsevier
... zero-copy **packet** capture, and efficient data analysis based on **application protocol** analysis and ... Then, to reduce the data load for **intrusion** analysis, RHPNIDS implements an ... Third, an **application-layer protocol** analysis and reassembling mechanism reduce the false alarm rate ...
Cited by 15 - Related articles

A high-level programming environment for **packet** trace anonymization and transformation
R Pang, V Paxson - Proceedings of the 2003 conference on ..., 2003 - portal.acm.org
... It is especially crippling for network **intrusion** detection research, forcing researchers to devise ... this work we develop a new method to allow anonymization of **packet** payloads as ... steps: 1. Payloads are reassembled and parsed to generate **application- protocol**-level, semantically ...
Cited by 140 - Related articles - BL Direct - All 23 versions

[PDF] Transport and **application protocol** scrubbing
GR Malan, D Watson, F Jahanian, P Howell - IEEE INFOCOM, 2000 - Citeseer
... scrub- bing mechanism: The protocol scrubber supports flexible transparent **application protocol** scrubbers that can ... attacks can utilize protocol ambiguities be- tween a network **intrusion** detection system ... attacks: insertion attacks, where the NID system accepts a **packet** that the ...
Cited by 70 - Related articles - View as HTML - BL Direct - All 26 versions

Network **intrusion** detection: Evasion, traffic normalization, and end-to-end protocol semantics
M Handley, V Paxson, C Kreibich - Proceedings of the 10th ..., 2001 - portal.acm.org
... the path of traffic into a site and patches up the **packet** stream to ... GR Malan, D. Watson, F. Jahanian and P. Howell, "Transport and **Application Protocol** Scrubbing", Proceedings ... Third International Workshop on the Recent Advances in **Intrusion** Detection (RAID 2000), Toulouse ...
Cited by 291 - Related articles - All 89 versions

Protocol analysis in **intrusion** detection using decision tree
T Abbes, A Bouhoula, M ... - ... Technology: Coding and ..., 2004 - ieeexplore.ieee.org
... Client Trace Server Trace Container : **Application protocol** Properties Next Container ... The trace will be then released when we finish the processing of the **packet**. ... 5 Conclusion Most **intrusion** detection systems rely on pattern match- ing operations to look for attack signatures. ...
Cited by 40 - Related articles - All 15 versions

[CITATION] **Intrusion** Detection Systems: An overview
B Goyal, S Sitaraman, S Krishnamurthy - SANS Institute, 2001
Cited by 4 - Related articles

Using CLIPS to detect network **intrusions**
P Alipio, P Carvalho, J Neves - Progress in Artificial Intelligence, 2003 - Springer
... In module EVENTS, actually the main module for all **intrusion** signatures, the ruleset is divided into several modules according to TCP/IP protocols. ... So, on level 3 several rulesets can be specified according to the **packet application protocol**. ...

Cited by 4 - Related articles - BL Direct - All 8 versions

[PDF] Statistical Analysis in Logs of DNS Traffic and E-mail Server
Y Musashi, R Matsuba, K ... - IPSJ SIG Notes, ..., 2003 - dua.cc.kumamoto-u.ac.jp
... Page 5. Statistical **Intrusion** Detection by DNS query Access Log of DNS query DNS ... **application protocol**, such as SMTP, POP3, FTP, ..., Ri = the network **application protocol**-based DNS query traffic, Ni = the traffic of i, mi = ... 1DNS: The DNS server and the DNS **packet** recorder. ...
Cited by 5 - Related articles - View as HTML - All 4 versions

Use of passive network mapping to enhance signature quality of misuse network **intrusion** dete systems
B Dayioglu, A Ozgit - ... of the Sixteenth International Symposium on ..., 2001 - Citeseer
... Citations. 551, Snort - Lightweight **Intrusion** Detection for Networks – Roesch - 1999. ... 13, Firewalking: A traceroute-like analysis of IP **packet** responses to determine gateway access control lists. http://www. ... 1, Transport and **Application Protocol** Scrubbing – al - 2000. ...
Cited by 16 - Related articles - Cached

Automatic Response to **Intrusion**
D Schnackenberg, H Holliday, T Reid, K Bunn, D ... - 2002 - oai.dtic.mil
... Details of the IDIP architecture, **application protocol**, and message protocol are contained in [1], [2], and [3 ... The IDIP **application layer protocol** coordinates **intrusion** tracking and isolation. ... Figure 2-3 through Figure 2-8 illustrate how IDIP accomplishes **intrusion** response. ...
Cited by 1 - Related articles - All 4 versions

[PDF] **Intrusion** Prevention Systems (IPS): next generation firewalls
P Lindstrom - Spire Research Report, ožujak, 2004 - castle.eiu.edu
... This means that **intrusion** prevention solutions are ideally positioned to deal with: ... Attack packets like those from LAND and WinNuke by using high-speed **packet** filters. ... by using **application protocol** rules and signatures. ...
Cited by 5 - View as HTML

Method and system for detecting unauthorized use of a communication network
P Abeni - US Patent App. 10/567,752, 2003 - Google Patents
... 0054] If the analysis process captures a **packet** coming from ... in a multi-tasking environment, in order to monitor more then one computer/**application**/**protocol** at the ... The different processes can run simulta- neously on the same **intrusion** detection system, involving different entities ...
All 4 versions

Design and Implementation of Protocol Analysis Sub-system in **Intrusion** Detection System [J]
LJXHP Armin - Computer Engineering and Applications, 2003 - en.cnki.com.cn
... Peking University,Beijing100871). Protocol analysis sub-system in **intrusion** detection system ... module,including parsing the header fields of a **packet**;context analysis ... application protocols analysis module,including abstracting keyword from **application protocol** messages.The ...
Cited by 7 - Related articles - Cached

A hybrid and hierarchical NIDS paradigm utilizing naive Bayes classifier
Q Zhao, J Sun, S Zhang - Canadian Conference on Electrical ..., 2004 - ieeexplore.ieee.org
... They customarily collect network **packet** and send the data to Payload Filter & Match module. ... of the protocol's normal pattern and also obtain the abnormal connection sequences pattern about a **application protocol** by simulating some **intrusion** procedure concerning ...
Cited by 1 - Related articles

The Research on Email Forensic Based Network
WQ Wang, WG Liu - icise, 1899 - computer.org
... The network **packet** is captured in linker layer, but Both the HTTP and SMTP used to carry email

is **Application layer protocol**, so it is impossible to get integrated email information from single network **packet**. ... Dispose plug-in Capture **packet** E-mail **Intrusion** QQ MSN .... 1913 ...
Related articles - All 3 versions

System and method for service tagging for enhanced **packet** processing in a network environm
RM Broberg, M Grayson, LF Menditto, RM ... - US Patent App. 10/ ..., 2004 - Google Patents
... an effective mapping between a source IP address of a given request **packet** and a ... to areas such as routing, security, accounting, firewalling, **intrusion** detection, **intrusion** prevention, filter ... CSPG 14 could be a wireless **application protocol** (WAP) gateway, a compres- sion and/or ...
All 2 versions

M-commerce security: the impact of wireless **application protocol** (WAP) security services on business and e-health solutions
J Tan, HJ Wen, T Gyires - International Journal of Mobile ..., 2003 - Inderscience
... The Wireless **Application Protocol** (WAP) is a specification for developing applications that integrate data ... To guard against **packet** sniffing and other unauthorised activities we have just discussed ... Authentication protocols and **intrusion** detection are also being put in place and ...
Cited by 19 - Related articles - All 7 versions

Attacking DDoS at the Source
JM Gregory, G Prier, P Reiher - ... of the IEEE International Conference on ..., 2002 - Citeseer
... 2002. 31, Transport and **application protocol** scrubbing – Malan, Watson, et al. - 2000. 7, Characterizing and Tracing **Packet** Floods Using Cisco Routers – Cisco. 4, NFR Network **Intrusion** Detection. http://www.nfr.com/products/NID – Security. ...
Cached - All 2 versions

A Policy Based Approach to Securing Egress Secure Socket Layer Connections on Local Area Networks
J Mathews, J Rowell, D Nadwodny, NAVAL ... - 2004 - oai.dtic.mil
... an SSL tunnel is established between two hosts, any sort of **application layer protocol** may be ... of the most popular methods of network defences: firewalls and **intrusion** detection systems. ... Standard **packet** filters and stateful inspection firewalls have no feature suitable to defend ...
Related articles - View as HTML - All 4 versions

[PDF] Traffic Analysis: from Stateful Firewall to Network **Intrusion** Detection System
F Guo, T Chiueh - RPE Report, January, 2004 - Citeseer
... Of course there are other ways to detect **intrusion**. ... If the signature is not in the beginning of the TCP segment, it is less likely that the signature exists in this **packet**. For **application** (**protocol**) recognition, we need to search for the signatures that can distinguish different protocols. ...
Cited by 4 - Related articles - View as HTML - All 5 versions

Protocol decode based stateful firewall policy definition language
PN Parmar, P Rajagopal, R ... - Fifth IEEE International ..., 2004 - ieeexplore.ieee.org
... SAFire employs extensive use of string manipulation functions for **application layer protocol** processing and ... The PAE was comprised of a **packet** header based classifier and the ... With the heterogeneity in firewall capabilities and **intrusion** detection systems being increasingly ...
Related articles - All 4 versions

A pattern-matching co-processor for network **intrusion** detection systems
CR Clark, DE Schimmel - 2003 IEEE International Conference ..., 2003 - ieeexplore.ieee.org
... by restricting the searching to a sub- section of a **packet** based on knowledge of the **application protocol**. ... The flow of data through the various components of the **intrusion** detection system is shown in Figure ... If a **packet** is part of a fragmented IP datagram, it is buffered until the full ...
Cited by 17 - Related articles - All 4 versions

Access control for networks
S Fan, S Truong - US Patent 6,219,706, 2001 - Google Patents
... Page 9. US Patent Apr. 17,2001 Sheet 8 of 11 US 6,219,706 Bl 512 Drop **packet**, reset the connection. Done. Is **Application Protocol** one of FTP, TFTP, RPC or SMTP? Does payload have an **Intrusion** Signature? Does the payload contain port negotiation command? ...
Cited by 21 - Related articles

Formal Design of **Packet** Filtering Systems
G Osman, MG Darwish, M Zaki - ...), May 7-9, 2002, Cairo, Egypt, 2002 - books.google.com
... TCP/IP protocol (Ether-header, IP-header, TCP-header, and the **application layer protocol** data). ... whole **packet** content (Ethernet-header, IP-header, TCP-header, and **application protocol**-data ... Mukherjee, L. Todd Heberlein, and Karl N. Levitt," Network **Intrusion** Detection", IEEE ...
Related articles - All 3 versions

[PDF] Enterprise Wide Web Application Security: An Introduction
E Karaarslan, T Tugluar, H Sengonca - 2004 - karaarslan.net
... can look deeper into sessions and can make drop/pass decisions based on **application-protocol** headers or ... In Step 4, the **packet** is received by the web server software. The **intrusion** is unsuccessful if the application designer has programmed the code with inspecting the input ...
Cited by 2 - Related articles - View as HTML - All 2 versions

[PDF] Balancing Privacy and Fidelity in **Packet** Traces for Security Evaluation
S Fahmy, C Tan - 2004 - cs.purdue.edu
... tool for sanitizing application payloads was introduced, which reassembles packets to obtain **application protocol** data, applies ... While one of the goals of that work was for testing **intrusion** detection systems ... If the original **packet** had incorrect values, either due to incorrect protocol ...
Cited by 1 - Related articles - View as HTML - All 2 versions

A security scheme for protecting security policies in firewall
JS Lee, JC Jeon, KY Yoo - ACM SIGOPS Operating Systems ..., 2004 - portal.acm.org
... will seemingly originate and terminate in the proxy, while the traffic through a **packet** filter will ... can be monitored and filtered on the basis of anything that the **application protocol** can identify ... in the best possible way and scrutinized regularly for anomalies or **intrusion** attempts [4 ...
Cited by 2 - Related articles - BL Direct - All 2 versions

[PDF] Improving Network Security Using Ntop
L Deri, S Suin - ... Recent Advances in **Intrusion** Detection (RAID 2000), 2000 - Citeseer
... **Application Protocol** Verification Intruders often exploit **application protocol** weakness for ... and V. Jacobson, The BSD Packer Filter: A New Architecture for User-level **Packet** Capture, Proceedings of ... [Mukherjee94] B. Mukherjee, and others, Network **intrusion** detection, IEEE ...
Cited by 12 - Related articles - View as HTML - All 24 versions

Access method and device for securing access to information system
D Fages, M Lafon, B Brodart - US Patent App. 10/537,310, 2003 - Google Patents
... data, as opposed to the information contained in the header of the **packet**, in order ... an "attack signature base" into them, as in the case of **intrusion** detection systems ... 2 3 4 computer telecommunication network access device 5 6 transported data **application protocol** transport ...
All 3 versions

A sequential pattern mining algorithm for misuse **intrusion** detection
SJ Song, Z Huang, HP Hu, SY Jin - Grid and Cooperative Computing-- ..., 2004 - Springer
... Protocol analysis reassembles network data stream and parses **application layer protocol**, and then detects attack with pattern ... At last, the attacker removes the **intrusion** trail. ... The method of character string matching in a **packet** and sensitive information Statistics cannot describe ...
Cited by 5 - Related articles - BL Direct - All 4 versions

Measuring normality in HTTP traffic for anomaly-based **intrusion** detection
JM Estévez-Tapiador, P García-Teodoro, JE Díaz- ... - Computer Networks, 2004 - Elsevier
... The incoming HTTP traffic is parameterised for evaluation on a **packet** payload basis. **...** traffic, of interest concerning anomaly detection; (b) a new anomaly-based **intrusion** detection approach that uses knowledge related to the **application-layer protocol** and improves **...**
Cited by 35 - Related articles - All 8 versions

Evaluation of the diagnostic capabilities of commercial **intrusion** detection systems
H Debar, B Morin - Recent Advances in **Intrusion** Detection, 2002 - Springer
... on evasion at the **application protocol** layer, because we believe that **application protocol** analysis is still an **...** Not only do we want to compare **intrusion**-detection products with each other, we also **...** These tests are related to low level manipulations of the IP **packet**, such as targa or **...**
Cited by 31 - Related articles - BL Direct - All 12 versions

IP network system having unauthorized **intrusion** safeguard function
T Ando, A Taguchi, T Kondou, H Kida - US Patent App. 09/848,691, 2001 - Google Patents
... Each of the plurality of border relay devices includes a discarding unit for discarding, if the IP **packet** forwarded is an unauthorized **intrusion packet**, this unauthorized **packet** when detecting a re-**intrusion** on the basis of filtering information for detect- ing the re-**intrusion** of the **...**
All 2 versions

[PDF] SIMULATING **INTRUSIONS** VIA SYNCHRONISING E-SECURITY METHODOLOGY ON GLOBAL WIRED-WIRELESS NETWORKS
G Williams - IWWST'04, 2004 - iwwst.org.uk
... work in conjunction with the Internet using protocols such as (WAP) Wireless **Application Protocol** Keen., Mackintosh **...** Techniques such as traffic analysis and **packet** sniffing could jeopardise the confidentiality of information **...** This could be interpreted as **intrusion** or interference. **...**
Related articles - View as HTML - All 3 versions

The network management design integrated with the **intrusion** detection system
XY Zhang, CZ Li, QG Hu - Proceedings of 2004 International ..., 2004 - ieeexplore.ieee.org
... connected, and sending the data packets to the detection engine module, where the data **packet** is compared with **...** It is a good way to adopt descriptive methods of the **intrusion** feature used by Snort **...** The rule set includes many "*.rules" files classed by **application layer protocol**. **...**
Cited by 1 - Related articles - All 3 versions

Software Rejuvenation Approach to Security Engineering
KMM Aung, JS Park - Computational Science and Its Applications-ICCSA . .., 2004 - Springer
... This transmission is termed as a request, even if in fact that **application protocol** being used **...** After analyzing the features of **intrusions** according to their state changes in transient period, we **...** In this section, we present our resolver can detect re- transmissions of a specific **packet**. **...**
Cited by 1 - Related articles - BL Direct

N3: A geometrical approach for network **intrusion** detection at the application layer
JM Estévez-Tapiador, P García-Teodoro, JE ... - ... Science and Its ... , 2004 - Springer
... Definition 1. A mathematical model of an **application-layer protocol** L, de- noted ML, is **...** Mahoney, MV, "Network Traffic Anomaly Detection Based on **Packet** Bytes", in Proceedings of **...** Verdejo, JE, "Stochastic Pro- tocol Modeling for Anomaly-Based Network **Intrusion** Detection", in **...**
Cited by 2 - Related articles - BL Direct - All 4 versions

[PDF] Realtime **intrusion**-forensics, a first prototype implementation
U Payer - TERENA Networking Conference, 2004 - Citeseer
... of already existing knowledge about state transitions, memory content, header information, and **packet** payload. **...** **Intrusion** detection should be an inherent service causing no extra charges **...** be treated in the same way by taking advantage of the **application protocol** state machines **...**

Cited by 4 - Related articles - View as HTML - All 3 versions

Internet security: a case study of firewall selection
HJ Wen, JHM Tarn - INFORMATION MANAGEMENT AND ..., 1998 - emeraldinsight.com
... Safeguards must be put in place to prevent **intrusion**, information theft, and "denial of service ... The device is used for examining the packets it receives - just like **packet** filters - but ... information, in-band, by using the existing connection within the bounds of the **application protocol**. ...
Cited by 3 - Related articles - BL Direct - All 6 versions

On the self-similarity of synthetic traffic for the evaluation of **intrusion** detection systems
WH Allen, GA Marin - 2003 - computer.org
... They made careful measurements of traffic characteristics (by **application protocol**) at several Air Force networks [5 ... Figure 1. **Packet** counts for each two-hour in- terval of the simulation days ... datasets could be used as a baseline for training anomaly-based **intrusion** detection sys ...
Cited by 17 - Related articles - All 5 versions

[CITATION] The Study and Implement of Content Audit System on High Speed Network
WANGGQIN Zhi-Guang, LIU Jin-De - Computer, 2003 - en.cnki.com.cn
... for load balancing and data distribution which is based on **application protocol** and session ... n 130012, China);Implementation of the keyword filter in the **packet** filter system ... Computer Science, Harbin Institute of Technology, Harbin 150001);Architecture of **Intrusion** Detection for ...
Cited by 1 - Related articles - Cached

State-driven stack-based network **intrusion** detection system
U Payer - Proceedings of the 7th International Conference on ..., 2003 - ieeexplore.ieee.org
... protocols) can also be treated in the same way, by taking advantage of **application protocol** state machines ... the callback-function is the response of the system if a potential **intrusion** is assumed. The header information of the IP-**packet** as well as higher level header information is ...
Cited by 1 - Related articles - All 2 versions

The Impact of Wireless **Application Protocol** (WAP) on M-Commerce Security
HJ Wen, T Gyires - Journal of Internet Commerce, 2002 - informaworld.com
... To guard against **packet** sniffing, the method most often adopted for the Internet ... **Protocol** Forum, (2001e), "Wireless Transport Layer Security, Ver- sion 6" Wireless **Application Protocol** Forum, (2001f ... Zhang, Y. and Lee, W. (2000), "**Intrusion** detection in wireless ad-hoc networks ...
Cited by 2 - Related articles - BL Direct - All 2 versions

Practical network security: experiences with ntop
L Deri, S Suin - Computer Networks, 2000 - Elsevier
... packets get lost and not to get stuck waiting for the lost **packet** to arrive. ... We are also running some experiments with WAP (Wireless **Application Protocol**) appliances [26] using the Nokia ... not only for traffic measurement and monitoring, but also as an **intrusion** detection system. ...
Cited by 11 - Related articles - All 32 versions

SQLrand: Preventing SQL injection attacks
SW Boyd, AD Keromytis - Applied Cryptography and Network Security, 2004 - Springer
... The prevalence of buffer overflow attacks [3,29] as an **intrusion** mechanism has resulted in considerable ... language of choice, MySQL provides many APIs to ac- cess the database, yet the same **application protocol**. ... The query **packet** carries the actual request to the database. ...
Cited by 121 - Related articles - BL Direct - All 16 versions

Policy management for network-based **intrusion** detection and prevention
YM Chen, Y Yang - IEEE/IFIP Network Operations and ..., 2004 - ieeexplore.ieee.org
... For example, we can block or replace **application protocol** commands embedded in **packet** payloads. ... transit from one to another as the **intrusion** aggravates. For example, we may start from

dropping **packet**, then blocking a source IP address, and finally transits into blocking the **...**
Cited by 15 - Related articles - All 2 versions

Method for generating filters designed to avoid risks of breach in interconnected computer netw
J Fougerat - US Patent 6,775,694, 2004 - Google Patents
... on the graphic interlace, by means ol arrow curves lor each **application protocol** previously selected **...** However, it also implies a share of hazards, network **intrusion** risks, 15 protection problems. There is hardware and software avail- able for performing **packet** filtering using the **...**
All 4 versions

[PDF] Firewall technologies
R Zalenski - IEEE potentials, 2002 - 140.130.175.70
... Its privacy needs to be secured when applicable. If a company's systems are compro- mised by malicious **intrusion**, the com- pany's ability to provide goods and ser- vices to their customers is impaired or halted. **...** 2. **Packet** filtering is the simplest firewall to implement. **...**
Cited by 39 - Related articles - View as HTML - BL Direct - All 4 versions

[PDF] An Architectural Framework for Distributed **Intrusion** Detection using Smart Agents
V Chatzigiannakis, G Androulidakis, M ... - ... of SAM04, Las Vegas, 2004 - netmode.ntua.gr
... The **application protocol** used is proprietary and is still under consideration. **...** is **packet** was probably part of a port scanning session. . **...** Th 4 Our distributed **Intrusion** Detection System may be optionally linked with the Distributed Cooperative Framework against DDoS attacks [12]. **...**
Cited by 2 - Related articles - View as HTML

[PDF] Going Beyond Behavior-Based **Intrusion** Detection
MR Hines - Dept. of Computer Science, Binghamton University, ..., 2003 - Citeseer
... The IPv6 **packet** would only need a small 16-bit space to reserve for **packet** source identification using **...** [5] Koral Ilgun, Richard A. Kemmerer, Phillip A. Porras. State Transition Analysis: A Rule-Based **Intrusion** Detection Approach. **...** Transport and **Application Protocol** Scrubbing. **...**
Cited by 1 - Related articles - View as HTML - All 6 versions

[PDF] Shaping the research agenda for security in e-commerce
R Oppliger - IEEE Proceedings of Tenth International Workshop on ..., 1999 - csl.mtu.edu
... In addition to "normal" **packet** filtering, stateful **...** mechanism, an appli- cation-level gateway (eg, a HTTP proxy server) un- derstands the **application protocol** being spoken **...** code (eg, Java applets, and ActiveX controls); • The use of security scanners and **intrusion** detection systems **...**
Cited by 9 - Related articles - View as HTML - All 5 versions

Learning nonstationary models of normal network traffic for detecting novel attacks
MV Mahoney, PK Chan - Proceedings of the eighth ACM SIGKDD ..., 2002 - portal.acm.org
... We have factored the **intrusion** detection problem into three terms: odds(attack), the **...** The attributes are the **application protocol** keywords, opening and closing TCP flags, source address, and **...** TCP stream to learn the allowable set of keywords for each **application layer protocol**. **...**
Cited by 210 - Related articles - All 15 versions

[PDF] CS424 Network Security: Bayesian Network **Intrusion** Detection (BNIDS)
K Johansen, S Lee - 2003 - Citeseer
... Although there are subtle variances in traffic and **packet** form, a well trained Bayesian model would be able to discern which of these **...** we have set out to provide a proof-of-concept BNIDS that may well validate the applicability of Bayesian techniques to **intrusion** detection. **...**
Cited by 2 - Related articles - View as HTML - All 4 versions

[PDF] 802.11 Network Deployment
T Karhima - 2004 - comlab.hut.fi
... **Application layer protocol** analysis **...** Measures and displays signal strength of all APs on all 14

DSSS channels as well as PERs (**Packet** Error Rates) and WEP encryption detection. **...** Kismet is an 802.11 layer2 wireless network detector, sniffer, and **intrusion** detection system. **...**
Related articles - View as HTML

[PDF] Network Working Group P. Srisuresh INTERNET-DRAFT Jasmine Networks Expires as o August 21, 2001 J. Kuthan GMD Fokus
J Rosenberg - 2001 - 64.170.98.42
... Intermediate Devices implementing policy based **packet** filtering, **intrusion** detection, load balancing, tunneling **...** Firewall is a policy based **packet** filtering Middlebox, typically used for **...** NAT device alone cannot provide the necessary **application/protocol** transparency in all cases **...**
Related articles - View as HTML - All 2 versions

Linux Systems as Network Infrastructure Components
T Mancill - Enterprise networking: multilayer switching and ..., 2002 - books.google.com
... example, **packet**-filtering rules can be set up as a combination of source IP address and destination port (indicating a particular Layer 4 **application protocol**, such as **...** Another area that will likely see growth is that of user-space **packet**- filters and **intrusion**-detection programs **...**
All 5 versions

Transparent communication management in wireless networks
D Kidston, JP Black, T Kunz - ... of the Seventh Workshop on Hot ..., 1999 - ieeexplore.ieee.org
... to the **packet** modifications of network address translators (NATs) [7]. NATs use **application**/ **protocol** knowledge to **...** this reason that protocol semantics can be main- tained without undue **intrusion** into the **...** The TTSF thus transparently modifies **packet** data so that each side of the **...**
Cited by 10 - Related articles - All 14 versions

Method and apparatus for permitting visualizing network data
C Newton, W Bird, D Spencer - US Patent App. 10/346,920, 2003 - Google Patents
... In one example, the types ol views include at least two olthe following: network address, **application**, **protocol**, flow type, **packet** type, geographic **...** Various network security software, such as firewalls, **Intrusion** Detection Systems (IDS), net- work monitors, and vulnerability **...**

Defending against flooding-based distributed denial-of-service attacks: A tutorial
RKC Chang - IEEE Communications Magazine, 2002 - ieeexplore.ieee.org
... can be exploited to launch reflector attacks, including TCP and UDP packets, various ICMP messages, and **application protocol** mes- sages. **...** this approach is effective only if ISP networks are willing to cooperate and to install **packet** filters upon receiving **intrusion** alerts. **...**
Cited by 278 - Related articles - BL Direct - All 26 versions

Dynamic, Cooperating Boundary Controllers
D Schnackenburg, BOEING DEFENSE AND SPACE ... - 2002 - oai.dtic.mil
... attacker's network (Figure 5), temporarily blocking selected traffic from the attacker's **packet** stream if **...** IDIP-Enabled = **Intrusion** Detection System IDIP-Enab@ed Inb□s@onDetect@on **...** 1.6.5 IDIP Application Layer The IDIP **application layer protocol** is responsible for initiating and **...**
Cited by 7 - Related articles - All 2 versions

Adaptive System Security Policies
D Sachnackenberg, K Bunn, D Darby, L Rockwell, T ... - 2002 - oai.dtic.mil
... For attacks such as the "Ping of Death" where a single **packet** can crash a target system, the best approach is prevention. **...** 2.1 IDIP Overview The IDIP **application layer protocol** coordinates **intrusion** tracking and isolation. **...**
All 3 versions

Adaptive System Security Policies
T Reid, K Bunn, D Sachnackenberg, D Darby, L ... - 2002 - Storming Media

... For attacks such as the "Ping of Death" where a single **packet** can crash a target system, the best approach is prevention. ... 2.1 IDIP Overview The IDIP **application layer protocol** coordinates **intrusion** tracking and isolation. ...

[PDF] Boundary detection in tokenizing network application payload for anomaly detection
R Vargiya, P Chan - Workshop on Data Mining for Computer Security, 2003 - Citeseer
... 1. Introduction Motivation: Traditional **intrusion** detection systems use misuse/signature detection, which ... Parsing **packet** headers is relatively simple as there are few commonly used ... Hard coding the parser for each **application protocol** could be time consuming, particularly when ...
Cited by 25 - Related articles - View as HTML - All 3 versions

SubSeven's Honey Pot Program
A Abimbola, D Gresty, Q Shi - Network Security, 2002 - Elsevier
... The above classifications are two complementary trends in **intrusion** detection. ... When SubSeven tries to connect with KillSwitch, it sends a sys **packet** that contains in the payload both a client and server IP and respective port ... Server Socket (main **application protocol** interface). ...
All 3 versions

Security in a Mobile World--is Bluetooth the Answer?
R Barber - Computers & Security, 2001 - Elsevier
... As the telecoms environment moves towards offering an IP-type **packet** switched service ... The use of Wireless **Application Protocol** (WAP) services for mobile phones and other mobile ... updates and patches when they are provided by manufacturers; and **intrusion** detection testing ...
Cited by 11 - Related articles - All 8 versions

List of acronyms
ANXAN Exchange, XML ebXML eBusiness, S ... - BT Technology ..., 2001 - Springer
... information assurance project IBIA International Biometric Industry Association IDS **intrusion** detection system ... certificate management protocol POT pyramid of trust PS **packet** switched PSTN ... Web Consortium WAN wide area network WAP wireless **application protocol** WIM WAP ...
All 2 versions

[PDF] Stateful inspection firewalls
C Roecki, CM Director - Juniper Networks White Paper, 2004 - abchost.sk
... For example, most enterprises combine a strong perimeter defense with **intrusion** detection and ... **Packet** filters used with firewalls typically include protocol type, IP address, and/or ... File Transfer Protocol (FTP) — An IETF standard **application protocol** for transferring files between ...
Cited by 4 - Related articles - View as HTML - All 16 versions

[PDF] Detecting novel attacks by identifying anomalous network packet headers
M Mahoney, P Chan - Florida Institute of Technology Technical Report ..., 1999 - Citeseer
... We got good performance because the important fields for **intrusion** detection have a small r, so ... For instance, Instead of listing all possible hashes of the IP **packet** length (0, 1, 2 ... to our unofficial classification) are shown in parenthesis, with the **application layer protocol** that those ...
Cited by 43 - Related articles - View as HTML - All 8 versions

Eliminating steganography in internet traffic with active wardens
G Fisk, M Fisk, C Papadopoulos, J Neil - Information Hiding, 2003 - Springer
... However, there have been several studies of ways to subvert **intrusion** detection systems using techniques known as **packet** evasion [29, 24] which exploit ambiguities in the semantics of network protocols and differences in perspective between **intrusion** detection sys- tems ...
Cited by 74 - Related articles - BL Direct - All 27 versions

Firewalls—Evolve or Die
DJ Gooch, SD Hubbard, MW Moore, J Hill - BT Technology Journal, 2001 - Springer

... A protocol tunnel can turn an **application layer protocol** (such as HTTP, or SMTP) into a transport layer protocol. ... viruses or **intrusions**. ... IPsec uses cryptography to provide authentication, integrity, confidentiality and replay protection at the **packet** level, and is a technology which ...
Cited by 8 - Related articles - BL Direct - All 4 versions

Alert transmission apparatus and method for policy-based **intrusion** detection and response
SY Yoon, GI Ahn, KY Kim, JS Jang - US Patent App. 10/448,414, 2003 - Google Patents
... transmission system during a fixed time is grouped into one **packet** and then ... protocols convey information between the PDF and the PEP, an **intrusion** detection exchange ... a blocks extensible exchange protocol (BEEP) corresponding to a general **application protocol** framework. ...

Protocol anomaly detection and verification
IS Yoo - ... Assurance Workshop, 2004. Proceedings from the ..., 2004 - ieeexplore.ieee.org
... layer protocol anomalies in layer-3 and layer- 4 and **application layer protocol** anomalies in ... Without names and prior documen- tation, understanding their **intrusion** methods and their effects can ... Then we present our **packet** verifier model, which includes a SanityChecker and an ...
Cited by 5 - Related articles

A Data Mining approach for building cost-sensitive and light **intrusion** detection models
NORTH CAROLINA STATE UNIV AT RALEIGH - 2004 - oai.dtic.mil
... We have factored the **intrusion** detection problem into three terms: odds(attack), the ... The attributes are the **application protocol** keywords, opening and closing TCP flags, source address, and ... TCP stream to learn the allowable set of keywords for each **application layer protocol**. ...
Related articles - View as HTML

[PDF] A machine learning approach to anomaly detection
PK Chan, MV Mahoney, MH Arshad - 2003 - Citeseer
... U nW = , we would like to estimate: P(W|U). For example, consider these network **packet** values: V ... In **intrusion** detection we experience that attacks cause bursty behavior as well ... To improve effectiveness and efficiency, CLAD learns a model for each port (**application protocol**). ...
Cited by 22 - Related articles - View as HTML - All 10 versions

GBF: a grammar based filter for Internet applications
M Zaki, MG Darwish, G Osman - Journal of Network and Computer ..., 2003 - Elsevier
... defines the different layers of the TCP/IP protocol (Ether-header, IP-header, TCP-header, and the **application layer protocol** data). ... The input of the **packet** filter, Fig. ... 3. Thus all fields for Ethernet-header, IP-header, TCP-header, and data part of the **application protocol** are defined. ...
Cited by 2 - Related articles - All 4 versions

[PDF] Broadband service gateway platform for readily available and reliable business applicatio and services
M Nishihara, S KAMIYA, T HAYASHI, H UENO, ... - NEC Journal of ..., 2004 - nec.co.jp
... 1) System security functions, such as **intrusion** detection/protection, an anti-virus function, and a firewall function. ... 1) The function to perform **packet** recognition and termination on the TCP/IP level. ... 4) The function to perform a part of the **application** (**protocol**) processing function. ...
Cited by 3 - Related articles - All 4 versions

System and method for covert management of passive network devices
P Evrard, O Naveau, S Nasdrovisky, O ... - US Patent App. 10/ ..., 2002 - Google Patents
... Network-based **intrusion** detection systems are often invisible, meaning that the network interface card ... to ASCII and back, as well as generic functions to build the **packet** that needs ... a detailed view of how each commu- nication layer transforms the **Application Protocol** Data Unit ...
Related articles - All 2 versions

[PDF] Bro: An open source network **intrusion** detection system

R Sommer - Proceedings of the 17. DFN-Arbeitstagung über ..., 2003 - Citeseer
... no assumption about the validity of the data is made during the **application-layer protocol** analysis. ... be restricted to a subset of packets by defining conditions the **packet** header has ... Bro's general approach to **intrusion** detection has a much broader scope than traditional signature ...
Cited by 11 - Related articles - View as HTML - All 6 versions

Method and apparatus for predictive and actual **intrusion** detection on a network
D Gassen, TP Donahue - US Patent App. 10/838,863, 2004 - Google Patents
... Accordingly, a need exists for software, systems and methods that can predict an **intrusion** detection and enable remedial action before a security breach ... When a **packet** that is scored above a specified threshold value is identified, at least one responsive action is implemented. ...

Internet security: firewalls and beyond
R Oppliger - Communications of the ACM, 1997 - portal.acm.org
... Since then, reports of security incidents, such as attempted and successful system **intrusions** and other ... proto- cols to build secure IP tunnels to other hosts, every IP **packet** sent to one ... that one might think of first is to modify each application (and **application protocol**) accordingly. ...
Cited by 128 - Related articles - BL Direct - All 4 versions

Characterization of defense mechanisms against distributed denial of service attacks
LC Chen, TA Longstaff, KM Carley - Computers & Security, 2004 - Elsevier
... Both firewall technology (Cheswick and Bellovin, 1994 and Zwicky et al., 2000) and **intrusion** detection systems (Axelsson, 2000, Debar et al ... The information may include network **packet** headers, **packet** rates of network flows/connections, or information on dropped packets. ...
Cited by 26 - Related articles - All 11 versions

[PDF] End-to-end web security—protocols overview
A Niemi - Department of Computer Science University of Helsinki ..., 2003 - Citeseer
... Firewalls and **intrusion** detection systems, for instance, help to maintain availability ... AH authenticates the entire inner IP **packet** and non-mutable portions of the outer IP ... SSL Handshake Protocol SSL Change Cipher Spec Protocol SSL Alert Protocol **Application Protocol** (eg HTTP ...
Cited by 2 - Related articles - View as HTML - All 4 versions

[PDF] Shomar: An open architecture for distributed **intrusion** detection services
J Undercoffer, F Perich, C Nicholas - University of Maryland, Baltimore ..., 2002 - Citeseer
... the IETF has proposed the **Intrusion** Detection Ex- change Protocol (IDXP) [7], an **application-layer protocol** for exchanging ... In SHOMAR, the notion of an **Intrusion** Detection (ID) Service is abstract, examples of ID services include, but are not limited to: a **packet** sniffing service ...
Cited by 11 - Related articles - View as HTML - All 5 versions

[PDF] Control networks and interoperability
HM Newman - Supplement to HPAC Engineering, 2001 - bacnet.org
... equipment intended for different purposes such as fire alarm, lighting control, **intrusion** detection, and ... workstation and digital controller that use BACnet/IP as their native **application protocol** via an ... Continuing down the stack, the UDP "**packet**" (the BAC- net/IP message with the ...
Cited by 5 - Related articles - View as HTML - BL Direct - All 3 versions

A security protocol intended to ease QoS management in IP networks
Y Shirashi, Y Fukuta, M Morii - ... and Communications in ..., 2004 - interscience.wiley.com
... (3) Destination protocol port: Port number on desti- nation host determined by **application protocol**. ... network environment for which the IPsec SPD is set appro- priately and **packet** filtering is ... to construct the network as an integrated system in which an **intrusion** detection system ...
Cited by 2 - Related articles - BL Direct - All 2 versions

[CITATION] Chapter List by Subject Area

D Nations, D Learning, EF Transfer, TV Enhanced, ... - The Internet ..., 2004 - Wiley
Related articles

Programmable context aware firewall with integrated **intrusion** detection system
P Rajagopal, R Sahita, PN Parmar - US Patent App. 10/815,539, 2004 - Google Patents
... Current firewall sys- tems generally lack integrated **intrusion** detection capability to match the ... [0089] In some embodiments, PAE 114 performs a second level of **packet** filtering that ... A flow belonging to any **application protocol** may be initiated, created and terminated typically ...

[PDF] A Software System for **Packet** Trace Customization with Application to NIDS Evaluation
A Rupp - Master's thesis, Universitat des ..., 2004 - net.informatik.tu-muenchen.de
... a system-independent interface for user-level **packet** cap- turing, enables the use of kernel-space **packet** filtering mechanisms (BPF [24]) and defines a standard format for trace files (pcap files). Because of these features all listed tools and several network **intrusion** detection sys ...
Cited by 2 - Related articles - View as HTML - All 9 versions

Eighth IEEE International Symposium on Computers and Communication
T Kemer-Antalya - 2003 - ieeexplore.ieee.org
... B. Crispo, and AS Tanenbaum NetHost-Sensor: A Novel Concept in **Intrusion** Detection Systems ... Dynamic Capacity Management for Voice-over-**Packet** Networks ... 1135 Teruyuki Hasegawa, Toru Hasegawa, and M. Lagreze Wireless **Application Protocol** Transport Layer ...

[PDF] Attacking DDoS at the source
P Reiher, J Mirkovic, G Prier - Proceedings of the 10th IEEE International ..., 2002 - Citeseer
... 1. Introduction Distributed denial-of-service attacks are comprised of **packet** streams from disparate sources. ... The flow is classified as an attack flow if its **packet** ratio is above the threshold; otherwise, it is considered a compliant flow. ICMP normal traffic model. ...
Cited by 14 - Related articles - View as HTML - All 26 versions

Fast and secure magnetic WORM storage systems
Y Wang, Y Zheng - 2003 - computer.org
... The **packet** vault: secure storage of network data. In: Proceedings of the USENIX Workshop on **Intrusion** Detection and Network Monitoring. ... http:// e2fsprogs.sourceforge.net/ext2intro.html [7] CITI. Projects: Advanced **Packet** Vault. ... Transport and **application protocol** scrubbing. ...
Cited by 7 - Related articles - All 11 versions

Web-based intelligent surveillance system for detection of criminal activities
ACM Fong, SC Hui - Computing & Control Engineering ..., 2001 - ieeexplore.ieee.org
... Remote monitoring Security monitoring systems are currently used mainly for **intrusion** detection and access ... data such as control information since it guarantees the delivery of every data **packet**. RTSP is an **application-layer protocol** for control of streaming media on the Internet ...
Cited by 19 - Related articles - BL Direct - All 6 versions

Internet security protocols
W Fumy - State of the Art in Applied Cryptography, 1998 - Springer
... However, while firewalls can guard against **intrusion** and unauthorized use, they can ... of transport layer security protocols is that they are **application protocol** independent and that ... authentication and encryption techniques and can protect any **application-layer protocol** such as ...
Cited by 2 - Related articles - BL Direct - All 4 versions

Progress in Internet Security
RJ Atkinson, JE Klinker - Advances in computers, 1999 - Elsevier
... The Web's Hyper-Text Transfer Protocol (HTTP) is an example of an **application layer protocol**. ... hosts now employ address-centric access control lists to reduce risk of **intrusions** [86]. Such **packet** filters commonly use the Source IP Address, Destination IP Address, upper-layer ...

Cited by 1 - Related articles - BL Direct - All 2 versions

System and method for accelerating cryptographically secured transactions
M Gast - US Patent App. 09/944,694, 2001 - Google Patents
... Providing **intrusion** detection for SSL sessions has not been a possibility until the advent ... [0013] Another problem with existing solutions is that the Wireless **Application Protocol** (WAP) suite ... illustrating conceptually an example of the contents of a network protocol **packet** that may ...

Distributed network security system and a hardware processor therefor
AA Pandya - US Patent App. 10/783,690, 2004 - Google Patents
... A scheduler schedules packets to **packet** processors for processing. ... SCSI Architecture Layers nitiatQCl/pSjjfisj'stern tar.get I/O system — Center) I 101- — •-. v(§jiifi!)ir; , 102- -^ SCSI Application S CSI Application Application Laye ri; SCSI **Application Protocol** Logical Unit (SCSI ...
All 4 versions

Method and apparatus for detecting **intrusions** on a computer system
RM Gupta, PK Jain, KE Amidon, F Gong, S ... - US Patent App. 10/ ..., 2002 - Google Patents
... Processor **Packet** Decoder Load Balancer Statistical Analysis and DDOS Detection Module Anomaly Detector Fixed-Field Detector Protocol Parser State Machines Tables Stream Orderer Token Detector Attack Detector Classification and Pattern-Matching Module **Intrusion** ...
All 2 versions

Extracting attack manifestations to determine log data requirements for **intrusion** detection
EL Barse, E Jonsson - Computer Security Applications ..., 2004 - ieeexplore.ieee.org
... These changed log entries are then used to flag malicious behaviour by an **intrusion** detection system. ... The elements in the network **packet** logs that were selected for comparison was source IP, destination IP, transport protocol, **application protocol** port, and data length. ...
Cited by 22 - Related articles - All 10 versions

Distributed Management of High-Layer Protocols and Network Services through a Programmat Agent-Based Architecture
L Gaspary, L Balbinot, R Storch, F Wendt, L ... - Networking—ICN ..., 2001 - Springer
... If the trace to be monitored belongs to a single **application-layer protocol** then the network manager may ... This feature is interesting, for in- stance, to observe the attempt of an **intrusion**. The example presented in figure 6 defines that every TCP **packet** must be tested for the ...
Cited by 7 - Related articles - BL Direct - All 7 versions

[PDF] Attack-Class-Based Analysis of **Intrusion** Detection Systems
D Alessandri - ... of Newcastle upon Tyne, Newcastle, UK, 2004 - homepage.swissonline.ch
... described thus far. This insight motivated this work, which aims to support the designers of IDSs in their 1 PDU: Protocol data unit; a **packet** 2 Page 13. ATTACK-CLASS-BASED ANALYSIS OF **INTRUSION** DETECTION SYSTEMS task. ...
Cited by 14 - Related articles - View as HTML - All 2 versions

Create email alert